МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Учебное пособие

для студентов, обучающихся по специальностям
21040665 «Сети связи и системы коммутаций»,
01020065 «Прикладная математика» и направлениям
21070062 «Инфокоммуникационные технологии и системы связи»,
01020062 «Прикладная математика»

Составители: Д. А. Капустин,
В. Е. Дементьев

Ульяновск
УлГТУ
2011

УДК 004.7 (075)
ББК 32.073.202 я7
И 74

Рецензенты: Заведующий кафедрой Телекоммуникационных систем МГТУ МИРЭА, д-р техн. наук, профессор В. И. Нефедов;

Ульяновский филиал ФГУП «ЦентрИнформ», руководитель удостоверяющего центра А. Е. Клочков

Утверждено редакционно-издательским советом университета в качестве учебного пособия

И 74 **Информационно-вычислительные сети** : учебное пособие / Д. А. Капустин, В. Е. Дементьев. – Ульяновск : УлГТУ, 2011. – 141с.

ISBN 978-5-9795-0926-6

Учебное пособие посвящено компьютерным сетям, даны основные понятия сетевой терминологии, описаны виды архитектуры, приводится описание топологии и методов доступа. Описаны основные компоненты ЛВС (сетевые адаптеры, сетевые операционные системы, сетевые службы и др.) и требования, предъявляемые к сетям. Концепция построения сетей представлена на основе семиуровневой базовой эталонной модели передачи данных в сетях (ISO). Даны понятия физической среды связи, линии связи и каналов связи, приведены типы физических сред передачи данных в сетях. Описаны популярные стеки протоколов, даются сведения по сетевому оборудованию.

Печатается в авторской редакции.

УДК 004.7 (075)
ББК 32.073.202 я7

ISBN 978-5-9795-0926-6

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ

АП – абонентский пункт

ИВС – информационно-вычислительная сеть

ЛВС – локальная вычислительная сеть

КС – компьютерная сеть

МПД – мультиплексор передачи данных

ОС – операционная система

ПК – персональный компьютер

ПО – программное обеспечение

СТД – система телеобработки данных

OSI – базовая эталонная модель взаимодействия открытых систем

ВВЕДЕНИЕ

Учебное пособие представляет собой введение в сетевую тематику и дает базовые знания по организации и функционированию сетей. В нем даны общие понятия компьютерных сетей, их структуры, сетевых компонентов. Здесь приведены виды топологии, используемые для физического соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных. Передача данных в сети рассматривается на базе эталонной базовой модели, разработанной Международной организацией по стандартам взаимодействия открытых сетей. Описываются правила и процедуры передачи данных между информационными системами. Приводятся типы сетевого оборудования, их назначение и принципы работы. Описывается сетевое программное обеспечение, используемое для организации сетей. Изучаются наиболее популярные сетевые операционные системы, их достоинства и недостатки. Рассматриваются принципы межсетевого взаимодействия.

Учебное пособие может быть использовано при изучении дисциплин «Информационно-вычислительные сети» и «Компьютерные сети и защита информации».

1. ОБЗОР И АРХИТЕКТУРА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

1.1. Основные определения и термины

Сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных. Международная организация по стандартизации определила вычислительную сеть *как последовательную бит-ориентированную передачу информации между связанными друг с другом независимыми устройствами* [1].

Сети обычно находятся в частном ведении пользователя и занимают некоторую территорию и по территориальному признаку разделяются на:

– Локальные вычислительные сети (ЛВС) или Local Area Network (LAN), расположенные в одном или нескольких близко расположенных зданиях. ЛВС обычно размещаются в рамках какой-либо организации (корпорации, учреждения), поэтому их называют корпоративными.

– Распределенные компьютерные сети, глобальные или Wide Area Network (WAN), расположенные в разных зданиях, городах и странах, которые бывают территориальными, смешанными и глобальными. В зависимости от этого глобальные сети бывают четырех основных видов: городские, региональные, национальные и транснациональные. В качестве примеров распределенных сетей очень большого масштаба можно назвать: Internet, EUNET, Relcom, FIDO.

В состав сети в общем случае включается следующие элементы:

– сетевые компьютеры (оснащенные сетевым адаптером);

– каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);

– различного рода преобразователи сигналов;

– сетевое оборудование.

Различают два понятия сети: *коммуникационная сеть* и *информационная сеть* (рис. 1.1).

Коммуникационная сеть предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.

Информационная сеть предназначена для хранения информации и состоит из *информационных систем*. На базе коммуникационной сети может быть построена группа информационных сетей.

Под *информационной системой* следует понимать систему, которая является поставщиком или потребителем информации.

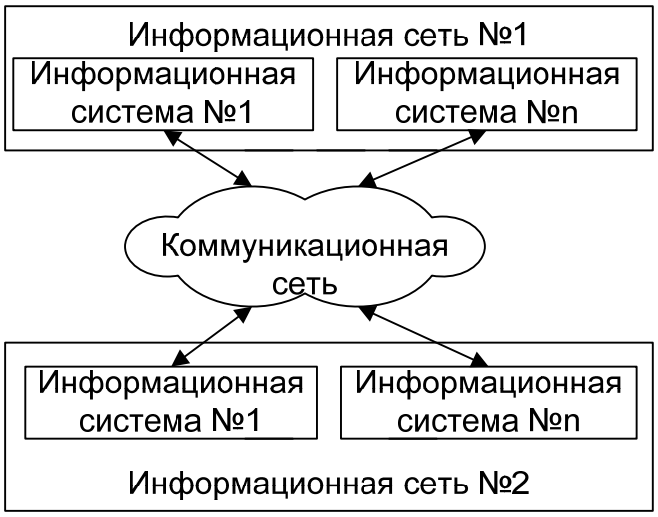

Рис. 1.1. Информационные и коммуникационные сети

Компьютерная сеть состоит из *информационных систем* и *каналов связи*.

Под *информационной системой* следует понимать объект, способный осуществлять хранение, обработку или передачу информация. В состав *информационной системы* входят: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных. В дальнейшем информационная система, предназначенная для решения задач пользователя, будет называться *рабочая станция (client)*. Рабочая станция в сети отличается от обычного персонального компьютера (ПК) наличием *сетевой карты* (*сетевого адаптера*), канала для передачи данных и сетевого программного обеспечения.

Под *каналом связи* следует понимать путь или средство, по которому передаются сигналы. Средство передачи сигналов называют *абонентским,* или *физическим, каналом*.

Каналы связи (data link) создаются по линиям связи при помощи сетевого оборудования и физических средств связи. Физические средства связи построены на основе витых пар, коаксиальных кабелей, оптических каналов или эфира. Между взаимодействующими информационными системами через физические каналы коммуникационной сети и узлы коммутации устанавливаются *логические каналы.*

Логический канал – это путь для передачи данных от одной системы к другой. Логический канал прокладывается по маршруту в одном или нескольких физических каналах. *Логический канал* можно охарактеризовать как маршрут, проложенный через физические каналы и узлы коммутации.

Информация в сети передается *блоками данных* по процедурам обмена между объектами. Эти процедуры называют *протоколами передачи данных.*

Протокол – это совокупность правил, устанавливающих формат и процедуры обмена информацией между двумя или несколькими устройствами.

Загрузка сети характеризуется параметром, называемым *трафиком*. *Трафик (traffic)* – это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих *блоков данных* и их длины, выраженное в битах в секунду.

Существенное влияние на характеристику сети оказывает *метод доступа*. *Метод доступа* – это способ определения того, какая из рабочих станций сможет следующей использовать канал связи и как управлять доступом к каналу связи (кабелю).

В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой *топологией*.

Топология – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. Тип топологии определяет производительность, работоспособность и надежность эксплуатации рабочих станций, а также время обращения к файловому серверу. В зависимости от топологии сети используется тот или иной метод доступа.

Состав основных элементов в сети зависит от ее архитектуры. *Архитектура* – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Архитектура определяет принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

В основном выделяют три вида архитектур: архитектура *терминал – главный компьютер*, архитектура *клиент – сервер* и *одноранговая* архитектура.

Современные сети можно классифицировать по различным признакам: по удаленности компьютеров, топологии, назначению, перечню предоставляемых услуг, принципам управления (централизованные и децентрализованные), методам коммутации, методам доступа, видам среды передачи, скоростям передачи данных и т. д.

1.2. Преимущества использования сетей

Компьютерные сети представляют собой вариант сотрудничества людей и компьютеров, обеспечивающего ускорение доставки и обработки информации.

Работы по созданию вычислительных сетей (ВС) начались еще в 60-х годах XX в. Прообразом ВС явились системы телеобработки данных (СТД), построенные на базе больших (а позже и миниЭВМ). В качестве средств передачи данных использовалась существующая

телефонная сеть. Структура СТД представлена на рис. 1.2. СТД состоит из абонентских пунктов (АП), модемов, мультиплексора передачи данных (МПД) и ЭВМ. Телефонная сеть ориентирована на передачу речевой (аналоговой) информации, поэтому одними из основных компонентов сети явились достаточно медленные аналоговые коммутаторы.

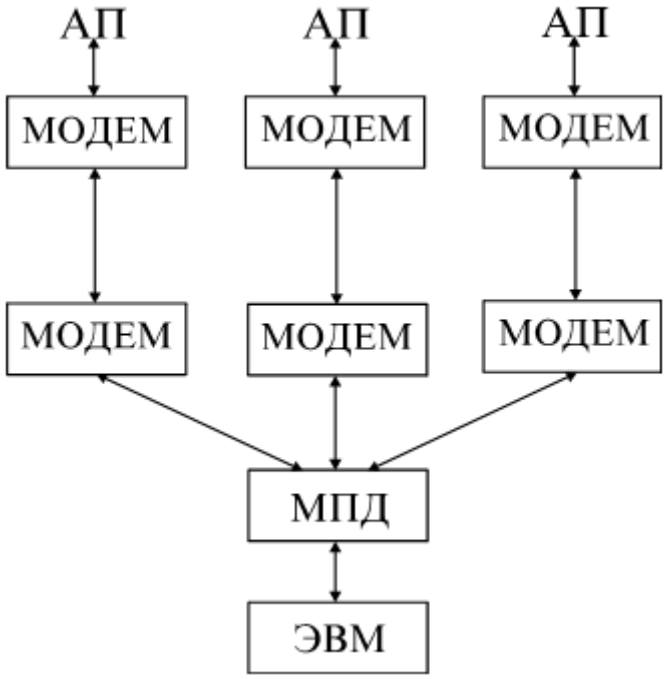

Рис. 1.2. Структура системы телеобработки данных

Основным недостатком СТД является невысокое быстродействие (9600 бит/с, реально 2400 бит/с). Поэтому одним из направлений совершенствования СТД явилась разработка *цифровых* телефонных коммутаторов. Аналоговую речь при этом предлагалось переводить в дискретную форму. Вторым существенным недостатком СТД является *возможность передачи данных по каналу связи в один и тот же момент времени только с одной скоростью*. Этот недостаток был преодолен использованием впервые в 70-х годах в США коммуникаций кабельного телевидения, позволяющих вести широкополосную передачу (ШП). ШП позволяет по одному кабелю вести передачу данных одновременно с различными скоростями. Третьим направлением перехода к сетям была разработка высокоскоростных

шин для обеспечения взаимодействия нескольких больших ЭВМ. Четвертым направлением развития ВС была реализация распределенной обработки данных. Для этого в середине 70-х годов появились технические средства и программное обеспечение, позволяющие связать ЭВМ в виде кольца или шины. В 80-х годах появились микроЭВМ. Существенно не отличаясь от больших и миниЭВМ по скорости обработки информации и объему ОП (оперативной памяти), микроЭВМ имели в десятки раз меньшую внешнюю память. Поэтому пятым направлением создания ИВС была разработка специальных дисковых мультиплексоров.

К середине 80-х годов все отмеченные тенденции развития сетей стали сближаться, что привело к разработке современных информационных сетей.

Соединенные в сеть компьютеры обмениваются информацией и совместно используют периферийное оборудование и устройства хранения информации (рис. 1.3). Основной целью создания компьютерных сетей является возможность совместного использования пользователями сети сетевых ресурсов. Под ресурсами ПК понимают любой из следующих элементов:

– логические диски;

– каталоги, файлы, прикладные программы, базы данных, текстовые процессоры;

– подключенные к ПК устройства (принтеры, модемы, сканеры и т. д.).

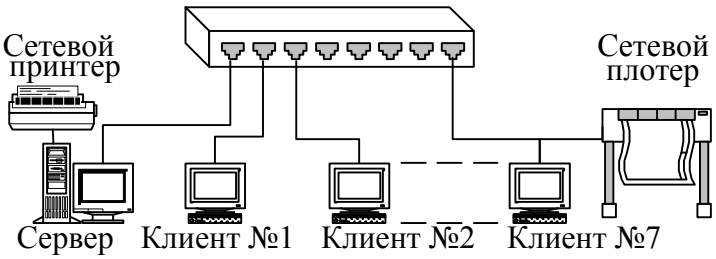

Рис. 1.3. Использование периферийного оборудования

Первые две группы перечисленных ресурсов являются информационными ресурсами, третья группа – технические ресурсы. Ресурсы, доступные только с персонального компьютера (ПК), на котором они находятся, называют *локальными.* Ресурсы ПК, доступные для других компьютеров сети, *называют разделяемыми,* или *сетевыми.*

Особую группу сетевых ресурсов представляет *разделяемое программное обеспечение* (ПО). Использование разделяемого ПО позволяет пользователям сети совместно использовать на нескольких машинах одну копию программного продукта, установленную на сервере или (в одноранговых сетях) на одной из машин. *Распределенное приложение* состоит из нескольких частей, каждая из которых выполняет определенную задачу на отдельном компьютере сети.

Главными преимуществами работы в сети являются возможность совместного доступа пользователей к сетевым ресурсам и возможность передачи данных между компьютерами без промежуточных носителей информации. Совместный доступ к информационным ресурсам позволяет во многих случаях избежать непроизводительного дублирования или разночтения одной и той же информации и экономить дисковое пространство. Совместный доступ к техническим ресурсам ПК дает возможность значительной экономии на приобретении периферийных устройств (принтеров, сканеров, модемов и т. д.). Использование сетей повышает производительность труда за счет значительной экономии времени, затрачиваемого на передачу информации между подразделениями и сотрудниками. Наконец, использование глобальных сетей, и, в частности, Internet, открывает практически неограниченные возможности коммуникации между пользователями ПК, находящимися в любой точке мира.

Можно использовать ЛВС как почтовую службу и рассылать служебные записки, доклады и сообщения другим пользователям.

1.3. Архитектура сетей

Компоновка и компоненты сети. «Сервер» и «рабочая станция»

Вычислительная сеть (ВС) – это сложный комплекс взаимосвязанных и согласованно функционирующих аппаратных и программных компонентов. Аппаратными компонентами локальной сети являются компьютеры и различное коммуникационное оборудование (кабельные системы, концентраторы и т. д.). Программными компонентами ВС являются операционные системы (ОС) и сетевые приложения.

Компоновкой сети называется процесс составления аппаратных компонентов с целью достижения нужного результата.

В зависимости от того, как распределены функции между компьютерами сети, они могут выступать в трех разных ролях:

1. Компьютер, занимающийся исключительно обслуживанием запросов других компьютеров, играет роль *выделенного сервера сети* (рис. 1.4).

2. Компьютер, обращающийся с запросами к ресурсам другой машины, играет роль *узла-клиента* (рис. 1.5).

3. Компьютер, совмещающий функции клиента и сервера, является *одноранговым узлом* (рис. 1.6).

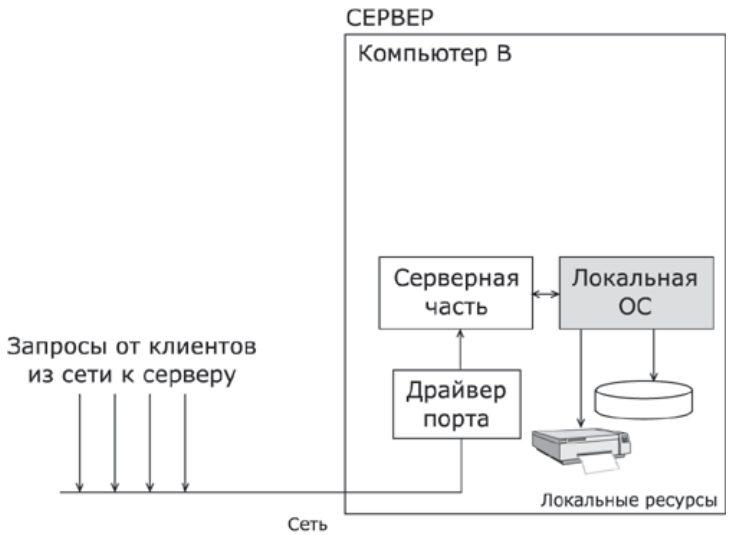

Рис. 1.4. Компьютер-выделенный сервер сети

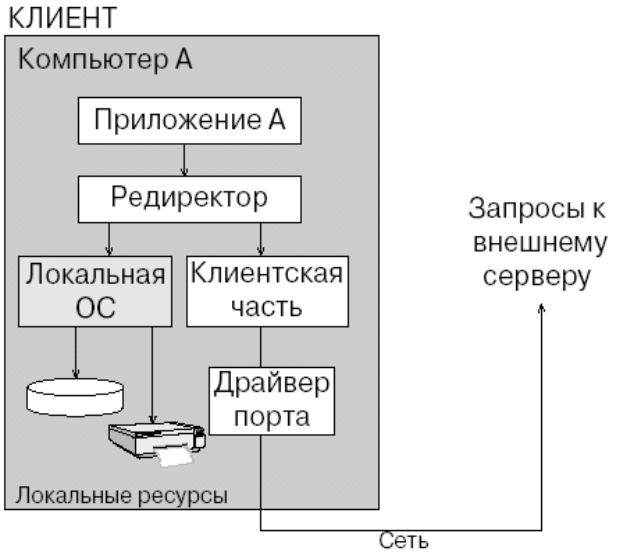

Рис. 1.5. Компьютер в роли узла-клиента

Очевидно, что сеть не может состоять только из клиентских или только из серверных узлов.

Сеть может быть построена по одной из трех схем:

- сеть на основе одноранговых узлов – одноранговая сеть;
- сеть на основе клиентов и серверов – сеть с выделенными серверами;
- сеть, включающая узлы всех типов – гибридная сеть.

Каждая из этих схем имеет свои достоинства и недостатки, определяющие их области применения.

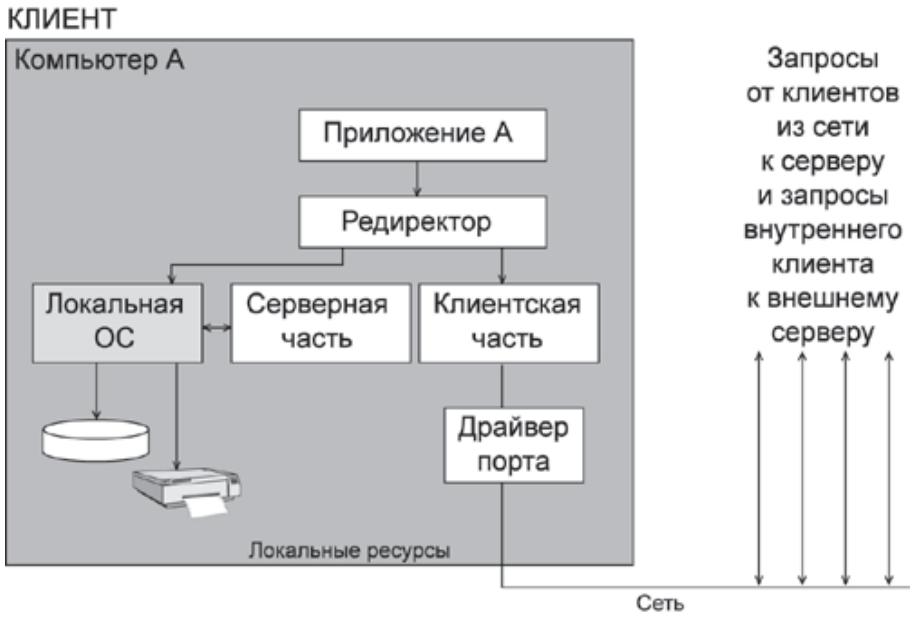

Рис. 1.6. Компьютер-одноранговый узел

В одноранговых сетях один и тот же ПК может быть и сервером, и клиентом, в том числе и клиентом своего клиента. В иерархических сетях разделяемые ресурсы хранятся только на сервере, сам сервер может быть клиентом только другого сервера более высокого уровня иерархии.

При этом каждый из серверов может быть реализован как на отдельном компьютере, так и в небольших по объему ЛВС, быть совмещенным на одном компьютере с каким-либо другим сервером.

Существуют и комбинированные сети, сочетающие лучшие качества одноранговых сетей и сетей на основе сервера. Многие администраторы считают, что такая сеть наиболее полно удовлетворяет их запросы.

Архитектура сети определяет основные элементы сети, характеризует ее общую логическую организацию, техническое обеспечение, программное обеспечение, описывает методы кодирования. Архитектура также определяет принципы функционирования и интерфейс пользователя.

Далее будет рассмотрено три вида архитектур:

- архитектура терминал-главный компьютер;
- одноранговая архитектура;
- архитектура клиент-сервер.

Архитектура терминал-главный компьютер

Архитектура терминал-главный компьютер (terminal-host computer architecture) – это концепция информационной сети, в которой вся обработка данных осуществляется одним или группой главных компьютеров.

Рассматриваемая архитектура предполагает два типа оборудования:

- главный компьютер, где осуществляется управление сетью, хранение и обработка данных;

– терминалы, предназначенные для передачи главному компьютеру команд на организацию сеансов и выполнения заданий, ввода данных для выполнения заданий и получения результатов.

Главный компьютер через МПД взаимодействуют с терминалами, как представлено на рис. 1.7.

Классический пример архитектуры сети с главными компьютерами – системная сетевая архитектура (System Network Architecture – SNA).

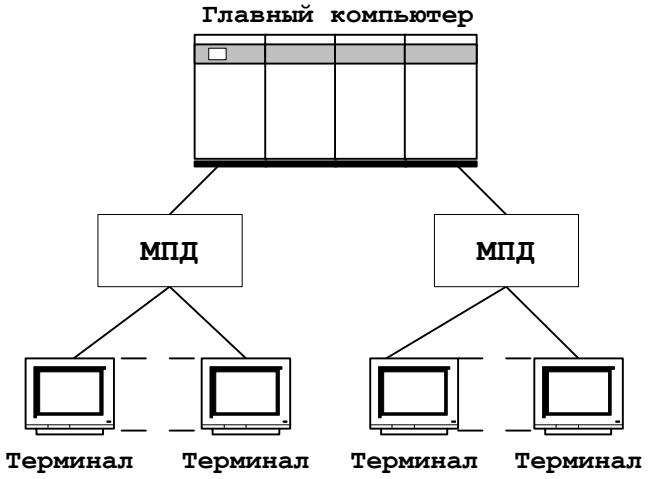

Рис. 1.7. Архитектура терминал-главный компьютер

Одноранговая архитектура

Одноранговая архитектура (peer-to-peer architecture) – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем системам. Данная архитектура характеризуется тем, что в ней все системы равноправны.

К *одноранговым* сетям относятся малые сети, где любая рабочая станция может выполнять одновременно функции файлового сервера и рабочей станции. В *одноранговых ЛВС* дисковое пространство и файлы на любом компьютере могут быть общими. Чтобы ресурс стал общим, его необходимо отдать в общее пользование, используя службы удаленного доступа сетевых одноранговых операционных систем. В зависимости от того, как будет установлена защита данных, другие пользователи смогут пользоваться файлами сразу же после их создания. *Одноранговые ЛВС* достаточно хороши только для небольших рабочих групп.

Одноранговые ЛВС являются наиболее легким и дешевым типом сетей для установки. При соединении компьютеров, пользователи могут предоставлять ресурсы и информацию в совместное пользование.

Одноранговые сети имеют следующие преимущества:

- они легки в установке и настройке;
- отдельные ПК не зависят от выделенного сервера;
- пользователи в состоянии контролировать свои ресурсы;
- малая стоимость и легкая эксплуатация;
- минимум оборудования и программного обеспечения;
- нет необходимости в администраторе;
- хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

Проблемой одноранговой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают виды *сервиса*, которые они предоставляли. Сетевую безопасность одновременно можно применить только к одному ресурсу, и пользователь должен помнить столько паролей, сколько сетевых ресурсов. При получении доступа к разделяемому ресурсу ощущается падение производительности компьютера. Существенным недостатком одноранговых сетей является отсутствие централизованного администрирования.

Использование одноранговой архитектуры не исключает применения в той же сети также архитектуры терминал-главный компьютер или архитектуры клиент-сервер.

Архитектура клиент-сервер

Архитектура клиент-сервер (client-server architecture) – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов (рис. 1.8). Рассматриваемая архитектура определяет два типа компонентов: *серверы и клиенты*.

Сервер – это объект, предоставляющий *сервис* другим объектам сети по их запросам. *Сервис* – это процесс обслуживания клиентов.

Сервер работает по заданиям клиентов и управляет выполнением их заданий. После выполнения каждого задания сервер посылает полученные результаты клиенту, пославшему это задание.

Сервисная функция в архитектуре клиент-сервер описывается комплексом прикладных программ, в соответствии с которым выполняются разнообразные прикладные процессы.

Рис. 1.8. Архитектура клиент-сервер

Процесс, который вызывает сервисную функцию с помощью определенных операций, называется *клиентом*. Им может быть программа или пользователь. На рис. 1.9 приведен перечень сервисов в архитектуре клиент-сервер.

Клиенты – это рабочие станции, которые используют ресурсы сервера и предоставляют удобные *интерфейсы пользователя*. *Интерфейсы пользователя* (рис. 1.9) – это процедуры взаимодействия пользователя с системой или сетью.

В *сетях с выделенным файловым сервером* на выделенном автономном *ПК* устанавливается серверная сетевая операционная система. Этот *ПК* становится *сервером.* ПО, установленное на рабочей станции, позволяет ей обмениваться данными с сервером. Наиболее распространенные сетевые операционная системы:

– NetWare фирмы Novel;
– Windows NT фирмы Microsoft;
– UNIX фирмы AT&T;
– Linux.

Помимо сетевой операционной системы необходимы сетевые прикладные программы, реализующие преимущества, предоставляемые сетью.

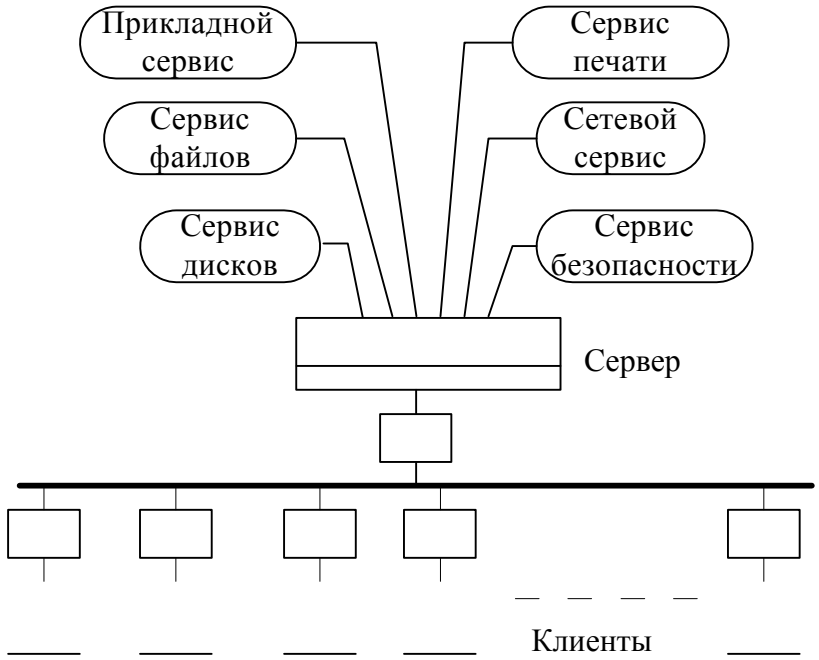

Рис. 1.9. Модель клиент-сервер

Круг задач, которые выполняют серверы в иерархических сетях, многообразен и сложен. Чтобы приспособиться к возрастающим потребностям пользователей, серверы в ЛВС стали специализированными. Так, например, в операционной системе Windows NT Server существуют различные типы серверов:

1. *Файл-серверы* и *принт-серверы.* Они управляют доступом пользователей к файлам и принтерам. Так, например, для работы с текстовым документом вы прежде всего запускаете на своем компьютере (PC) текстовый процессор. Далее требуемый документ текстового процессора, хранящийся на файл-сервере, загружается в память PC, и таким образом Вы можете работать с этим документом на

РС. Другими словами, файл-сервер предназначен для хранения файлов и данных.

2. *Серверы приложений* (в том числе сервер баз данных (БД), WEB-сервер). На них выполняются прикладные части клиент серверных приложений (программ). Эти серверы принципиально отличаются от файл-серверов тем, что при работе с файл-сервером нужный файл или данные целиком копируются на запрашивающий РС, а при работе с сервером приложений на РС пересылаются только результаты запроса. Например, по запросу можно получить только список работников, родившихся в сентябре, не загружая при этом в свою РС всю базу данных персонала.

3. *Почтовые серверы* управляют передачей электронных сообщений между пользователями сети.

4. *Факс-серверы* управляют потоком входящих и исходящих факсимильных сообщений через один или несколько факс-модемов.

5. *Коммуникационные серверы* управляют потоком данных и почтовых сообщений между данной ЛВС и другими сетями или удаленными пользователями через модем и телефонную линию. Они же обеспечивают доступ к Internet.

6. *Сервер служб каталогов* предназначен для поиска, хранения и защиты информации в сети. Windows NT Server объединяет РС в логические группы-домены, система защиты которых наделяет пользователей различными правами доступа к любому сетевому ресурсу.

Клиент является инициатором и использует электронную почту или другие сервисы сервера. В этом процессе клиент запрашивает вид обслуживания, устанавливает сеанс, получает нужные ему результаты и сообщает об окончании работы.

Сети на базе серверов имеют лучшие характеристики и повышенную надежность. Сервер владеет главными ресурсами сети, к которым обращаются остальные рабочие станции.

В современной клиент-серверной архитектуре выделяется четыре группы объектов: клиенты, серверы, данные и сетевые службы. Клиенты располагаются в системах на рабочих местах пользователей. Данные в основном хранятся в серверах. Сетевые службы являются совместно используемыми серверами и данными. Кроме того службы управляют процедурами обработки данных.

Сети клиент-серверной архитектуры имеют следующие преимущества:

– позволяют организовывать сети с большим количеством рабочих станций;

– обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;

– эффективный доступ к сетевым ресурсам;

– пользователю нужен один пароль для входа в сеть и для получения доступа ко всем ресурсам, на которые распространяются права пользователя.

Наряду с преимуществами сети клиент-серверной архитектуры имеют и ряд недостатков:

– неисправность сервера может сделать сеть неработоспособной;

– требуют квалифицированного персонала для администрирования;

– имеют более высокую стоимость сетей и сетевого оборудования.

Выбор архитектуры сети

Выбор архитектуры сети зависит от назначения сети, количества рабочих станций и от выполняемых на ней действий.

Следует выбрать одноранговую сеть, если:

– количество пользователей не превышает десяти;

– все машины находятся близко друг от друга;

– имеют место небольшие финансовые возможности;

– нет необходимости в специализированном сервере, таком как сервер БД, факс-сервер или какой-либо другой;

– нет возможности или необходимости в централизованном администрировании.

Следует выбрать клиент-серверную сеть, если:

– количество пользователей превышает десять;

– требуется централизованное управление, безопасность, управление ресурсами или резервное копирование;

– необходим специализированный сервер;

– нужен доступ к глобальной сети;

– требуется разделять ресурсы на уровне пользователей.

1.4. Семиуровневая модель OSI

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standardization Organization) разработала базовую модель связи открытых систем OSI (Open System Interconnection) [4]. Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни, прикладные процессы и физические средства соединения. На рис. 1.10 представлена структура базовой модели.

Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем.

Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам.

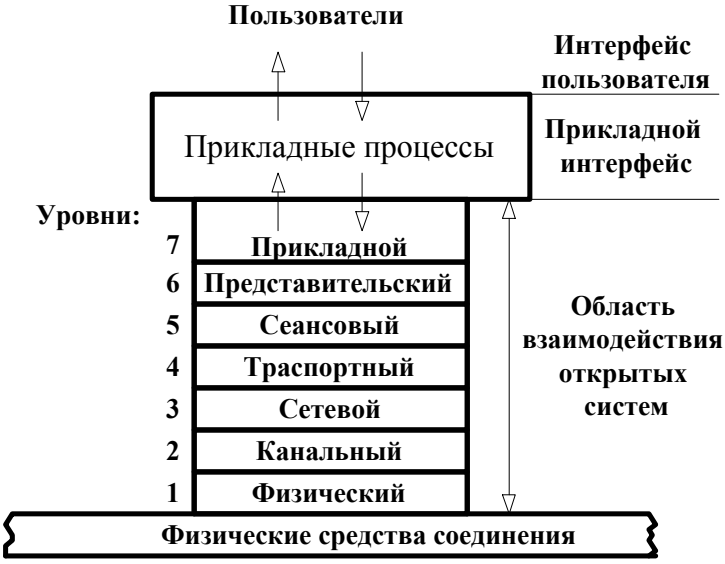

Рис. 1.10. Модель OSI

Если приложение может взять на себя функции некоторых верхних уровней модели OSI, то для обмена данными оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

Взаимодействие уровней модели OSI

Модель OSI можно разделить на две различных модели, как показано на рис. 1.11:

– горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;

– вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

Каждый уровень компьютера-отправителя взаимодействует с таким же уровнем компьютера-получателя, как будто он связан напрямую. Такая связь называется логической или виртуальной связью. В действительности взаимодействие осуществляется между смежными уровнями одного компьютера.

Итак, информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по физической среде до

компьютера-получателя и опять проходит сквозь все слои, пока не доходит до того же уровня, с которого она была послана на компьютере-отправителе.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной модели соседние уровни обмениваются данными с использованием интерфейсов прикладных программ API (Application Programming Interface).

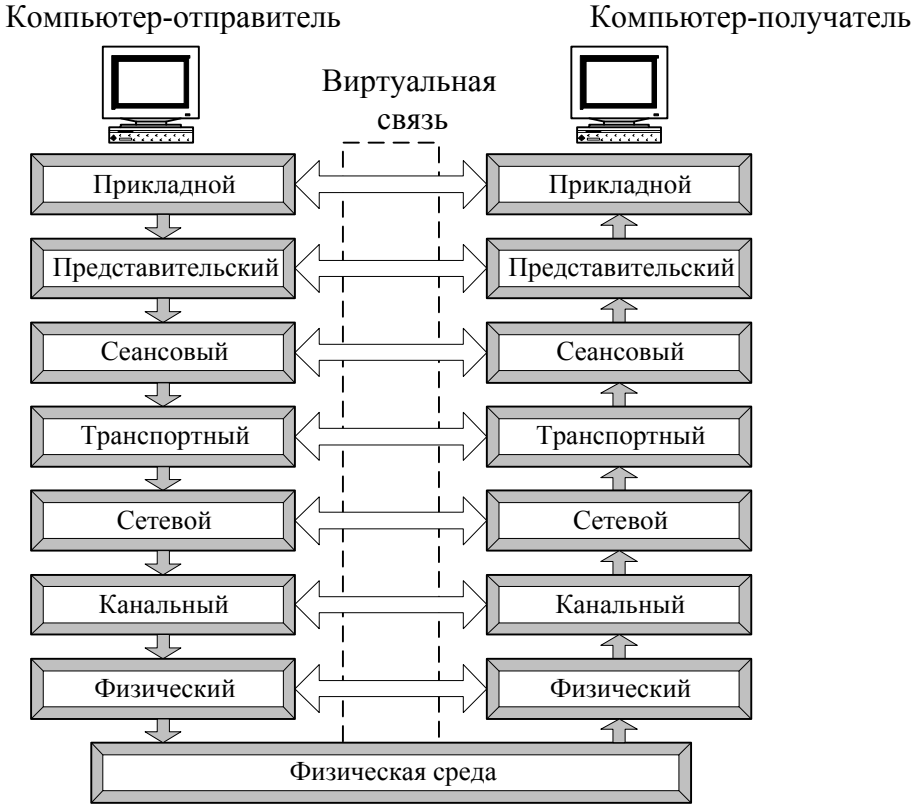

Рис. 1.11. Схема взаимодействия компьютеров в базовой эталонной модели OSI

Перед подачей в сеть данные разбиваются на пакеты. Пакет (packet) – это единица информации, передаваемая между станциями сети.

При отправке данных пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется управляющая информация данного уровня (заголовок), которая необходима для успешной передачи данных по сети, как это показано на рис. 1.12, где *Заг* – заголовок пакета, *Кон* – конец пакета.

На принимающей стороне пакет проходит через все уровни в обратном порядке. На каждом уровне протокол этого уровня читает

информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню. Когда пакет дойдет до *Прикладного* уровня, вся управляющая информация будет удалена из пакета, и данные примут свой первоначальный вид.

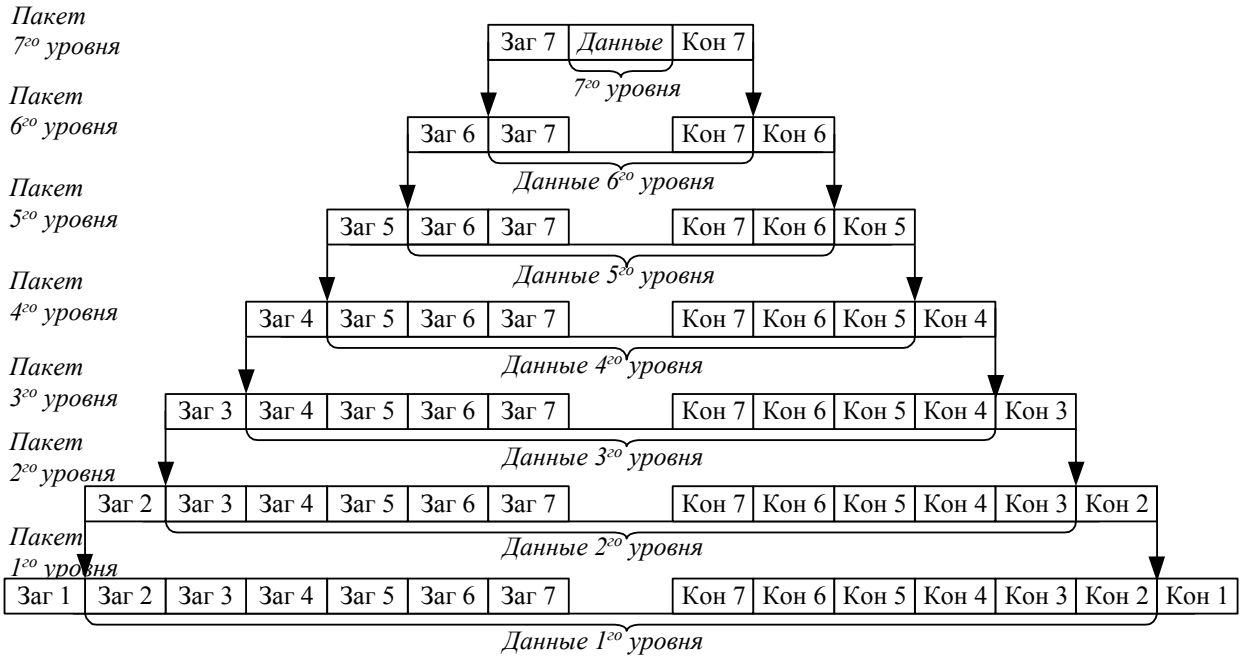

Рис. 1.12. Формирование пакета каждого уровня семиуровневой модели

Каждый уровень модели выполняет свою функцию. Чем выше уровень, тем более сложную задачу он решает.

Отдельные уровни модели *OSI* удобно рассматривать как *группы программ*, предназначенных для выполнения конкретных *функций*. Один уровень, к примеру, отвечает за обеспечение преобразования данных из *ASCII* в *EBCDIC* и содержит *программы*, необходимые для выполнения этой задачи.

Каждый уровень обеспечивает сервис для вышестоящего уровня, запрашивая в свою очередь сервис у нижестоящего уровня. Верхние уровни запрашивают сервис почти одинаково: как правило, это требование маршрутизации каких-то данных из одной сети в другую. Практическая реализация принципов адресации данных возложена на

нижние уровни. На рис. 1.13 приведено краткое описание функций всех уровней.

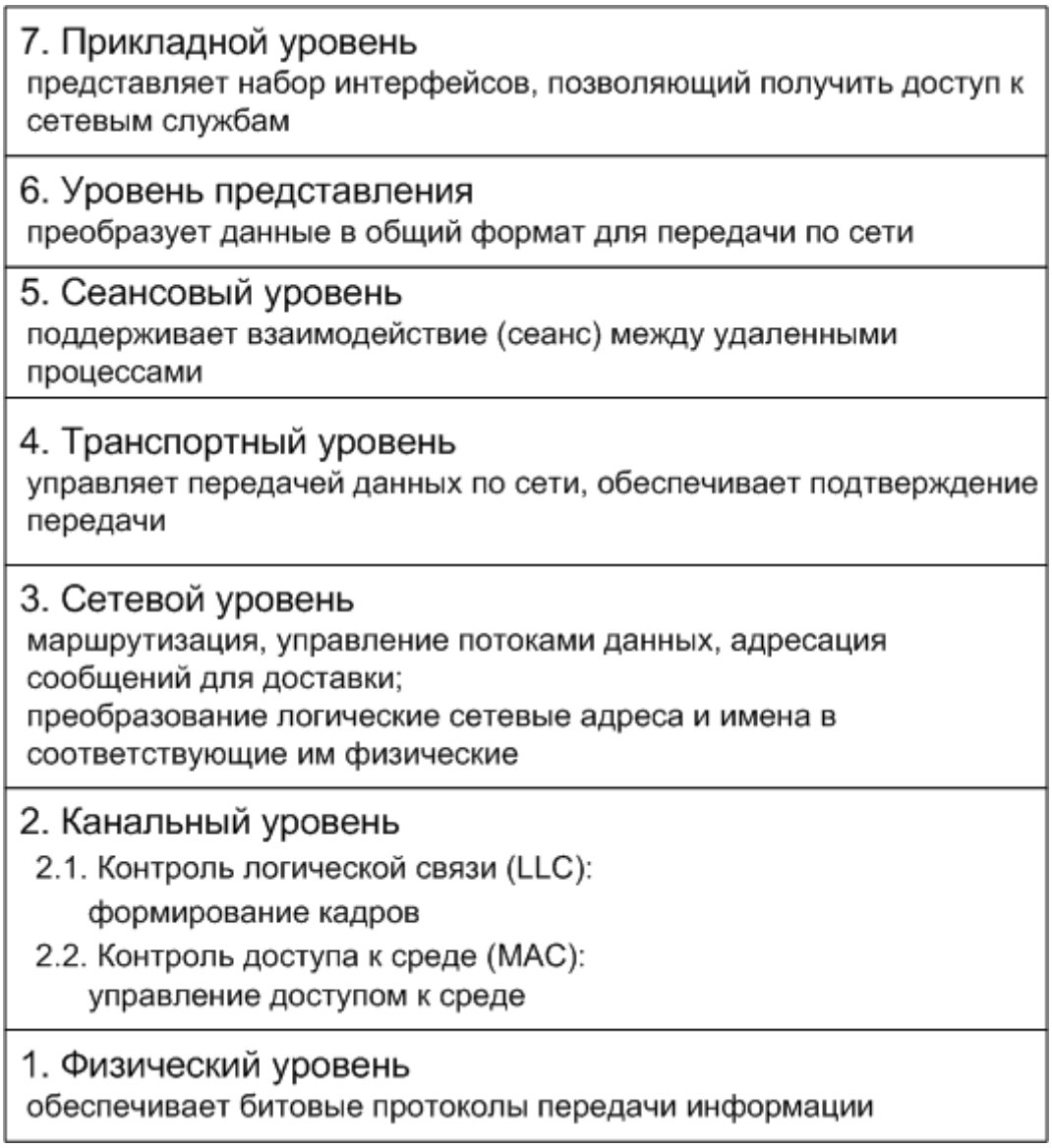

Рис. 1.13. Функции уровней модели OSI

Рассматриваемая модель определяет взаимодействие открытых систем разных производителей в одной сети. Поэтому она выполняет для них координирующие действия по:

- взаимодействию прикладных процессов;
- формам представления данных;
- единообразному хранению данных;
- управлению сетевыми ресурсами;
- безопасности данных и защите информации;
- диагностике программ и технических средств.

Прикладной уровень (Application layer)

Прикладной уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам.

В действительности прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например с помощью протокола электронной почты. Специальные элементы прикладного сервиса обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Если, например программе необходимо переслать файлы, то обязательно будет использован *протокол передачи, доступа и управления файлами* FTAM (File Transfer, Access, and Management). В модели OSI *прикладная программа*, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные в виде *Дейтаграммы* на *прикладной уровень*. Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы, другими словами, какой вид должен принять данный запрос.

Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

Прикладной уровень выполняет следующие функции:

1. Выполнение различных видов работ.
   - передача файлов;
   - управление заданиями;
   - управление системой и т. д.;
2. Идентификация пользователей по их паролям, адресам, электронным подписям;
3. Определение функционирующих абонентов и возможности доступа к новым прикладным процессам;
4. Определение достаточности имеющихся ресурсов;

5. Организация запросов на соединение с другими прикладными процессами;

6. Передача заявок представительскому уровню на необходимые методы описания информации;

7. Выбор процедур планируемого диалога процессов;

8. Управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов;

9. Определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок);

10. Соглашение об исправлении ошибок и определении достоверности данных;

11. Согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

Указанные функции определяют виды сервиса, которые прикладной уровень предоставляет прикладным процессам. Кроме этого, прикладной уровень передает прикладным процессам сервис, предоставляемый физическим, канальным, сетевым, транспортным, сеансовым и представительским уровнями.

На *прикладном уровне* необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское программное обеспечение.

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних трех уровней относятся:

– FTP (File Transfer Protocol) протокол передачи файлов;

– TFTP (Trivial File Transfer Protocol) простейший протокол пересылки файлов;

– X.400 электронная почта;

– Telnet работа с удаленным терминалом;

– SMTP (Simple Mail Transfer Protocol) простой протокол почтового обмена;

– CMIP (Common Management Information Protocol) общий протокол управления информацией;

– SLIP (Serial Line IP) IP для последовательных линий. Протокол последовательной посимвольной передачи данных;

– SNMP (Simple Network Management Protocol) простой протокол сетевого управления;

– FTAM (File Transfer, Access, and Management) протокол передачи, доступа и управления файлами.

Уровень представления данных (Presentation layer)

Функции данного уровня – представление данных, передаваемых между прикладными процессами, в нужной форме.

Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе. В случаях необходимости уровень представления в момент передачи информации выполняет преобразование форматов данных в некоторый общий формат представления, а в момент приема, соответственно, выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Такая ситуация может возникнуть в ЛВС с неоднотипными компьютерами (*IBM PC* и *Macintosh*), которым необходимо обмениваться данными. Так, в полях баз данных информация должна быть представлена в виде букв и цифр, а зачастую и в виде графического изображения. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой.

В основу общего представления данных положена единая для всех уровней модели система ASN.1. Эта система служит для описания структуры файлов, а также позволяет решить проблему шифрования данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена

данными обеспечивается сразу для всех прикладных сервисов. Примером такого протокола является протокол *Secure Socket Layer (SSL),* который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня.

Представительный уровень выполняет следующие основные функции:

1. Генерация запросов на установление сеансов взаимодействия прикладных процессов.
2. Согласование представления данных между прикладными процессами.
3. Реализация форм представления данных.
4. Представление графического материала (чертежей, рисунков, схем).
5. Засекречивание данных.
6. Передача запросов на прекращение сеансов.

Протоколы уровня представления данных обычно являются составной частью протоколов трех верхних уровней модели.

Сеансовый уровень (Session layer)

Сеансовый уровень – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами.

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Сеансовый уровень управляет передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят в *координации связи* между двумя прикладными программами, работающими на разных рабочих станциях. Это происходит в виде хорошо структурированного диалога. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:

– *полудуплексной* (процессы будут передавать и принимать данные по очереди);

– *дуплексной* (процессы будут передавать данные, и принимать их одновременно).

В полудуплексном режиме сеансовый уровень выдает тому процессу, который начинает передачу, *маркер данных*. Когда второму процессу приходит время отвечать, маркер данных передается ему. Сеансовый уровень разрешает передачу только той стороне, которая обладает маркером данных.

Сеансовый уровень обеспечивает выполнение следующих функций:

1. Установление и завершение на сеансовом уровне соединения между взаимодействующими системами.
2. Выполнение нормального и срочного обмена данными между прикладными процессами.
3. Управление взаимодействием прикладных процессов.
4. Синхронизация сеансовых соединений.
5. Извещение прикладных процессов об исключительных ситуациях.

6. Установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки.

7. Прерывание в нужных случаях прикладного процесса и его корректное возобновление.

8. Прекращение сеанса без потери данных.

9. Передача особых сообщений о ходе проведения сеанса.

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью протоколов трех верхних уровней модели.

Транспортный уровень (Transport Layer)

Транспортный уровень предназначен для передачи пакетов через коммуникационную сеть. На транспортном уровне пакеты разбиваются на блоки.

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Транспортный уровень определяет адресацию физических устройств (систем, их частей) в сети. Этот уровень гарантирует

доставку блоков информации адресатам и управляет этой доставкой. Его главной задачей является обеспечение эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность прохождения пакетов. Если проходит дубликат принятого ранее сообщения, то данный уровень опознает это и игнорирует сообщение.

В функции транспортного уровня входят:

1. Управление передачей по сети и обеспечение целостности блоков данных.
2. Обнаружение ошибок, частичная их ликвидация и сообщение о неисправленных ошибках.
3. Восстановление передачи после отказов и неисправностей.
4. Укрупнение или разделение блоков данных.
5. Предоставление приоритетов при передаче блоков (нормальная или срочная).
6. Подтверждение передачи.
7. Ликвидация блоков при тупиковых ситуациях в сети.

Начиная с транспортного уровня, все вышележащие протоколы реализуются программными средствами, обычно включаемыми в состав сетевой операционной системы.

Наиболее распространенные протоколы транспортного уровня включают в себя:

– TCP (Transmission Control Protocol) протокол управления передачей стека TCP/IP;

– UDP (User Datagram Protocol) пользовательский протокол дейтаграмм стека TCP/IP;

– NCP (NetWare Core Protocol) базовый протокол сетей NetWare;

– SPX (Sequenced Packet eXchange) упорядоченный обмен пакетами стека Novell;

– TP4 (Transmission Protocol) – протокол передачи класса 4.

Сетевой уровень (Network Layer)

Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути.

Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку виртуальных каналов между ними. *Виртуальный* или *логический канал* – это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках. Сообщения сетевого уровня принято называть *пакетами* (packet). В них помещаются фрагменты данных. Сетевой уровень отвечает за их адресацию и доставку.

Прокладка наилучшего пути для передачи данных называется *маршрутизацией*, и ее решение является главной задачей сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

Протокол канального уровня обеспечивает доставку данных между любыми узлами только в сети с соответствующей *типовой топологией*. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами.

Таким образом, внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается

сетевой уровень. При организации доставки пакетов на сетевом уровне используется понятие *номер сети.* В этом случае *адрес* получателя состоит из *номера сети* и *номера компьютера* в этой сети.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. *Маршрутизатор* – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз, выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

Сетевой уровень отвечает за деление пользователей на группы и маршрутизацию пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

Сетевой уровень выполняет функции:

1. Создание сетевых соединений и идентификация их портов.
2. Обнаружение и исправление ошибок, возникающих при передаче через коммуникационную сеть.
3. Управление потоками пакетов.
4. Организация (упорядочение) последовательностей пакетов.
5. Маршрутизация и коммутация.
6. Сегментирование и объединение пакетов.

На сетевом уровне определяется два вида протоколов. Первый вид относится к определению *правил передачи пакетов* с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых *протоколами обмена маршрутной*

информацией. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений.

Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Наиболее часто на сетевом уровне используются протоколы:

– IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию;

– IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;

– X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2);

– CLNP (Connection Less Network Protocol) сетевой протокол без организации соединений.

Канальный уровень (Data Link)

Единицей информации канального уровня являются *кадры (frame)*. Кадры – это логически организованная структура, в которую можно помещать данные. Задача канального уровня – передавать кадры от сетевого уровня к физическому уровню.

На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок.

Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит, в начало и конец каждого кадра, чтобы отметить его, а также вычисляет контрольную

сумму, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка.

Задача канального уровня – брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи.

На этом же уровне определяются правила использования физического уровня узлами сети. Электрическое представление данных в ЛВС (биты данных, методы кодирования данных и маркеры) распознаются на этом и только на этом уровне. Здесь обнаруживаются и исправляются (путем требований повторной передачи данных) ошибки.

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Спецификации IEEE 802.X делят канальный уровень на два подуровня:

– *LLC* (*Logical Link Control*) управление логическим каналом осуществляет логический контроль связи. Подуровень LLC обеспечивает обслуживание сетевого уровня и связан с передачей и приемом пользовательских сообщений.

– *MAC* (*Media Assess Control)* контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера или обнаружение коллизий или столкновений) и управляет доступом к каналу связи. Подуровень *LLC* находится выше подуровня *MAC.*

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу.

При больших размерах передаваемых блоков данных канальный уровень делит их на кадры и передает кадры в виде последовательностей.

При получении кадров уровень формирует из них переданные блоки данных. Размер блока данных зависит от способа передачи, качества канала, по которому он передается.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

Канальный уровень может выполнять следующие виды функций:

1. Организация (установление, управление, расторжение) канальных соединений и идентификация их портов.
2. Организация и передача кадров.
3. Обнаружение и исправление ошибок.
4. Управление потоками данных.
5. Обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

Наиболее часто используемые протоколы на канальном уровне включают:

– HDLC (High Level Data Link Control) протокол управления каналом передачи данных высокого уровня, для последовательных соединений;

– IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x;

– Ethernet сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей частоты и обнаружением конфликтов;

– Token ring сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;

– FDDI (Fiber Distributed Date Interface Station) сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;

– X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов;

– Frame relay сеть, организованная из технологий X25 и ISDN.

Физический уровень (Physical Layer)

Физический уровень предназначен для сопряжения с *физическими средствами соединения*. *Физические средства соединения* – это совокупность *физической среды*, аппаратных и программных средств, обеспечивающая передачу сигналов между системами.

Физическая среда – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц.

Физический уровень состоит из *Подуровня стыковки со средой* и *Подуровня преобразования передачи.*

Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами. Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

– тип кабелей и разъемов;
– разводку контактов в разъемах;
– схему кодирования сигналов для значений 0 и 1.

Физический уровень выполняет следующие функции:

1. Установление и разъединение физических соединений.
2. Передача сигналов в последовательном коде и прием.
3. Прослушивание, в нужных случаях, каналов.
4. Идентификация каналов.
5. Оповещение о появлении неисправностей и отказов.

Оповещение о появлении неисправностей и отказов связано с тем, что на физическом уровне происходит обнаружение определенного класса событий, мешающих нормальной работе сети (столкновение кадров, посланных сразу несколькими системами, обрыв канала, отключение питания, потеря механического контакта и т.д.). Виды сервиса, предоставляемого канальному уровню, определяются протоколами физического уровня. Прослушивание канала необходимо в тех случаях, когда к одному каналу подключается группа систем, но одновременно передавать сигналы разрешается только одной из них. Поэтому прослушивание канала позволяет определить, свободен ли он для передачи. В ряде случаев для более четкого определения структуры физический уровень разбивается на несколько подуровней. Например, физический уровень беспроводной сети делится на три подуровня (рис. 1.14).

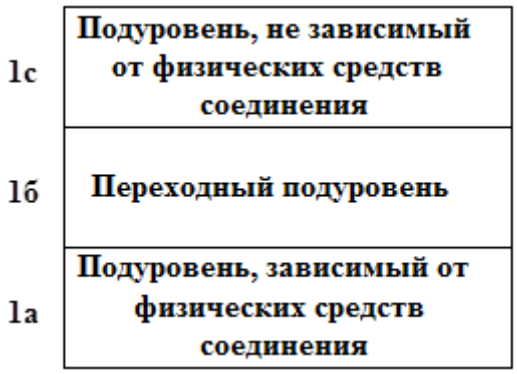

Рис. 1.14. Физический уровень беспроводной локальной сети

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером. Повторители являются единственным типом оборудования, которое работает только на физическом уровне.

Физический уровень может обеспечивать как асинхронную (последовательную) так и синхронную (параллельную) передачу, которая применяется для некоторых мэйнфреймов и мини-компьютеров. На физическом уровне должна быть определена схема кодирования для представления двоичных значений с целью их передачи по каналу связи. Во многих локальных сетях используется манчестерское кодирование.

Примером протокола физического уровня может служить спецификация 10Base-T технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную витую пару категории 3 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100 метров, манчестерский код для представления данных и другие характеристики среды и электрических сигналов.

К числу наиболее распространенных спецификаций физического уровня относятся:

– EIA-RS-232-C, CCITT V.24/V.28 – механические/электрические характеристики несбалансированного последовательного интерфейса;

– EIA-RS-422/449, CCITT V.10 – механические, электрические и оптические характеристики сбалансированного последовательного интерфейса;

– Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;

– Token ring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера.

1.5. Контрольные вопросы

1. Дать определение сети.
2. Чем отличается коммуникационная сеть от информационной сети?
3. Как разделяются сети по территориальному признаку?
4. Что такое информационная система?
5. Что такое каналы связи?
6. Дать определение физического канала связи.
7. Дать определение логического канала связи.
8. Как называется совокупность правил обмена информацией между двумя или несколькими устройствами?
9. Как называется объект, способный осуществлять хранение, обработку или передачу данных, в состав, которого входят компьютер, программное обеспечение, пользователи и др. составляющие, предназначенные для процесса обработки и передачи данных?
10. Каким параметром характеризуется загрузка сети?
11. Что такое метод доступа?
12. Что такое совокупность правил, устанавливающих процедуры и формат обмена информацией?
13. Чем отличается рабочая станция в сети от обычного персонального компьютера?
14. Какие элементы входят в состав сети?
15. Как называется описание физических соединений в сети?
16. Что такое архитектура сети?
17. Как назвать способ определения, какая из рабочих станций сможет следующей использовать канал связи?
18. Перечислить преимущества использования сетей.
19. Чем отличается одноранговая архитектура от клиент-серверной архитектуры?
20. Каковы преимущества крупномасштабной сети с выделенным сервером?
21. Какие сервисы предоставляет клиент-серверная архитектура?

22. Преимущества и недостатки архитектуры терминал-главный компьютер.
23. В каком случае используется одноранговая архитектура?
24. Что характерно для сетей с выделенным сервером?
25. Как называются рабочие станции, которые используют ресурсы сервера?
26. Что такое сервер?
27. Что такое OSI?
28. Каково назначение базовой модели взаимодействия открытых систем?
29. На какие уровни разбита базовая модель OSI?
30. Какие функции несет уровень в модели взаимодействия открытых систем?
31. На какие единицы разбивается информация для передачи данных по сети?
32. Что обеспечивает горизонтальная составляющая модели взаимодействия открытых систем?
33. Какие элементы являются основными элементами для базовой модели взаимодействия открытых систем?
34. Какие функции выполняются на физическом уровне?
35. Какие вопросы решаются на физическом уровне?
36. Какой уровень модели OSI преобразует данные в общий формат для передачи по сети?
37. Какое оборудование используется на физическом уровне?
38. Какие известны спецификации физического уровня?
39. Перечислить функции канального уровня.
40. Какие функции канального уровня?
41. На какие подуровни разделяется канальный уровень и каковы их функции?
42. Функцией какого уровня является засекречивание и реализация форм представления данных?
43. Какие протоколы используются на канальном уровне?

44. Какое оборудование используется на канальном уровне?
45. Какие функции выполняются и какие протоколы используются на сетевом уровне?
46. Какое оборудование используется на сетевом уровне?
47. Перечислите функции транспортного уровня.
48. Какие протоколы используются на транспортном уровне?
49. Перечислить оборудование транспортного уровня.
50. Дать определение сеансового уровня.
51. Какой уровень отвечает за доступ приложений в сеть?
52. Задачи уровня представления данных.
53. Перечислить функции прикладного уровня.

2. СТАНДАРТЫ И СТЕКИ ПРОТОКОЛОВ

2.1. Спецификации стандартов

Спецификации Institute of Electrical and Electronics Engineers IEEE802 определяют стандарты для физических компонентов сети. Эти компоненты – сетевая карта (Network Interface Card – NIC) и сетевой носитель (network media), которые относятся к физическому и канальному уровням модели OSI [4]. Спецификации IEEE 802 определяют механизм доступа адаптера к каналу связи и механизм передачи данных. Стандарты IEEE802 подразделяют канальный уровень на подуровни:

– Logical Link Control (LLC) – подуровень управления логической связью;

– Media Access Control (MAC) – подуровень управления доступом к устройствам.

Спецификации IEEE 802 делятся на двенадцать стандартов:

802.1

Стандарт 802.1 (Internetworking – объединение сетей) задает механизмы управления сетью на MAC-уровне. В разделе 802.1 приводятся основные понятия и определения, общие характеристики и требования к локальным сетям, а также поведение маршрутизации на канальном уровне, где логические адреса должны быть преобразованы в их физические адреса и наоборот.

802.2

Стандарт 802.2 (Logical Link Control – управление логической связью) определяет функционирование подуровня LLC на канальном уровне модели OSI. LLC обеспечивает интерфейс между методами доступа к среде и сетевым уровнем.

802.3

Стандарт 802.3 (Ethernet Carrier Sense Multiple Access with Collision Detection – CSMA/CD LANs Ethernet – множественный доступ к сетям Ethernet с проверкой несущей и обнаружением конфликтов) описывает физический уровень и подуровень MAC для сетей, использующих шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов. Прототипом этого метода является метод доступа стандарта Ethernet (10BaseT, 10Base2, 10Base5). Метод доступа CSMA/CD. 802.3 также включает технологии Fast Ethernet (100BaseTx, 100BaseFx).

Этот метод доступа используется в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения – это один из факторов, определивших успех стандарта Ethernet. Кабель, к которому подключены все станции, работает в режиме *коллективного доступа (multiply access – MA).*

Метод доступа CSMA/CD определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети.

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.

802.4

Стандарт 802.4 (Token Bus LAN – локальные сети Token Bus) определяет метод доступа к шине с передачей маркера, прототип – ArcNet.

При подключении устройств в ArcNet применяют топологию «шина» или «звезда». Адаптеры ArcNet поддерживают метод доступа Token Bus (маркерная шина) и обеспечивают производительность 2,5 Мбит/с. Этот метод предусматривает следующие правила:

– все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);

– в любой момент времени только одна станция в сети обладает таким правом;

– кадр, передаваемый одной станцией, одновременно анализируется всеми остальными станциями сети.

В сетях ArcNet используется асинхронный метод передачи данных (в сетях Ethernet и Token Ring применяется синхронный метод), т. е. передача каждого байта в ArcNet выполняется посылкой ISU (Information Symbol Unit – единица передачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных.

802.5

Стандарт 802.5 (Token Ring LAN – локальные сети Token Ring) описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.

Сети стандарта Token Ring, так же как и сети Ethernet, используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему используется не случайный алгоритм, как в сетях Ethernet, а детерминированный, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование

кольца передается с помощью кадра специального формата, называемого маркером, или токеном.

802.6

Стандарт 802.6 (Metropolitan Area Network – городские сети) описывает рекомендации для региональных сетей.

802.7

Стандарт 802.7 (Broadband Technical Advisory Group – техническая консультационная группа по широковещательной передаче) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

802.8

Стандарт 802.8 (Fiber Technical Advisory Group – техническая консультационная группа по оптоволоконным сетям) содержит обсуждение использования оптических кабелей в сетях 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть FDDI (Fiber Distributed Data Interface).

Стандарт FDDI использует оптоволоконный кабель и доступ с применением маркера. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. Скорость сети до 100 Мб/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

802.9

Стандарт 802.9 (Integrated Voice and Data Network – интегрированные сети передачи голоса и данных) задает архитектуру и

интерфейсы устройств одновременной передачи данных и голоса по одной линии, а также содержит рекомендации по гибридным сетям, в которых объединяют голосовой трафик и трафик данных в одной и той же сетевой среде.

802.10

В стандарте 802.10 (Network Security – сетевая безопасность) рассмотрены вопросы обмена данными, шифрования, управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.

802.11

Стандарт 802.11 (Wireless Network – беспроводные сети) описывает рекомендации по использованию беспроводных сетей.

802.12

Стандарт 802.12 описывает рекомендации по использованию сетей 100VG – AnyLAN со скоростью 100Мб/с и методом доступа по очереди запросов и по приоритету (Demand Priority Queuing – DPQ, Demand Priority Access – DPA).

Технология 100VG – это комбинация *Ethernet* и *Token-Ring* со скоростью передачи 100 Мбит/с, работающая на неэкранированных витых парах. В проекте 100Base-VG усовершенствован метод доступа с учетом потребности мультимедийных приложений. В спецификации *100VG* предусматривается поддержка волоконно-оптических кабельных систем. Технология *100VG* использует метод доступа – обработка запросов по приоритету (demand priority access). В этом случае узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, а затем разрешает этот запрос в соответствии с приоритетом. Имеется два уровня приоритетов – высокий и низкий.

2.2. Протоколы и стеки протоколов

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется *стеком протоколов*. Для каждого уровня определяется набор функций–запросов для взаимодействия с вышележащим уровнем, который называется *интерфейсом*. Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются *протоколами*.

Существует достаточно много стеков протоколов, широко применяемых в сетях. Примерами популярных стеков протоколов могут служить стек IPX/SPX фирмы Novell, стек TCP/IP, используемый в сети Internet и во многих сетях на основе операционной системы UNIX, стек OSI международной организации по стандартизации, стек DECnet корпорации Digital Equipment и некоторые другие.

Стеки протоколов разбиваются на три уровня:

- сетевые;
- транспортные;
- прикладные.

Сетевые протоколы

Сетевые протоколы предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде. Ниже приведены наиболее популярные сетевые протоколы.

– **DDP** (Datagram Delivery Protocol – Протокол доставки дейтаграмм). Протокол передачи данных Apple, используемый в Apple Talk.

– **IP** (Internet Protocol – Протокол Internet). Протокол стека TCP/IP, обеспечивающий адресную информацию и информацию о маршрутизации.

– **IPX** (Internetwork Packet eXchange – Межсетевой обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для маршрутизации и направления пакетов.

– **NetBEUI** (NetBIOS Extended User Interface – расширенный пользовательский интерфейс базовой сетевой системы ввода вывода). Разработанный совместно IBM и Microsoft, этот протокол обеспечивает транспортные услуги для **NetBIOS.**

Транспортные протоколы

Транспортные протоколы предоставляют услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы.

– **ATP** (Apple Talk Protocol – Транзакционный протокол Apple Talk) и **NBP** (Name Binding Protocol – Протокол связывания имен). Сеансовый и транспортный протоколы Apple Talk.

– **NetBIOS** (Базовая сетевая система ввода вывода). NetBIOS устанавливает соединение между компьютерами, а **NetBEUI** предоставляет услуги передачи данных для этого соединения.

– **SPX** (Sequenced Packet eXchange – Последовательный обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для обеспечения доставки данных.

– **TCP** (Transmission Control Protocol – Протокол управления передачей). Протокол стека TCP/IP, отвечающий за надежную доставку данных.

Прикладные протоколы

Прикладные протоколы отвечают за взаимодействие приложений. Ниже приведены наиболее популярные прикладные протоколы.

– **AFP** (Apple Talk File Protocol – Файловый протокол Apple Talk). Протокол удаленного управления файлами Macintosh.

– **FTP** (File Transfer Protocol – Протокол передачи файлов). Протокол стека TCP/IP, используемый для обеспечения услуг по передачи файлов.

– **NCP** (NetWare Core Protocol – Базовый протокол NetWare). Оболочка и редиректоры клиента Novel NetWare.

– **SNMP** (Simple Network Management Protocol – Простой протокол управления сетью). Протокол стека TCP/IP, используемый для управления и наблюдения за сетевыми устройствами.

– **HTTP** (Hyper Text Transfer Protocol) – протокол передачи гипертекста и другие протоколы.

2.3. Стек протоколов OSI

Следует различать стек протоколов OSI и модель OSI (рис. 2.1). Стек OSI – это набор вполне конкретных спецификаций протоколов, образующих согласованный стек протоколов. Этот стек протоколов поддерживает правительство США в своей программе GOSIP. Стек OSI в отличие от других стандартных стеков полностью соответствует модели взаимодействия OSI и включает спецификации для всех семи уровней модели взаимодействия открытых систем.

На *физическом и канальном уровнях* стек OSI поддерживает спецификации Ethernet, Token Ring, FDDI, а также протоколы LLC, X.25 и ISDN.

На *сетевом* уровне реализованы протоколы, как без установления соединений, так и с установлением соединений.

Транспортный протокол стека OSI скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают нужное качество обслуживания независимо от нижележащего сетевого уровня. Чтобы обеспечить это, транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания. Определены 5 классов транспортного сервиса, от низшего класса 0 до высшего класса 4,

которые отличаются степенью устойчивости к ошибкам и требованиями к восстановлению данных после ошибок.

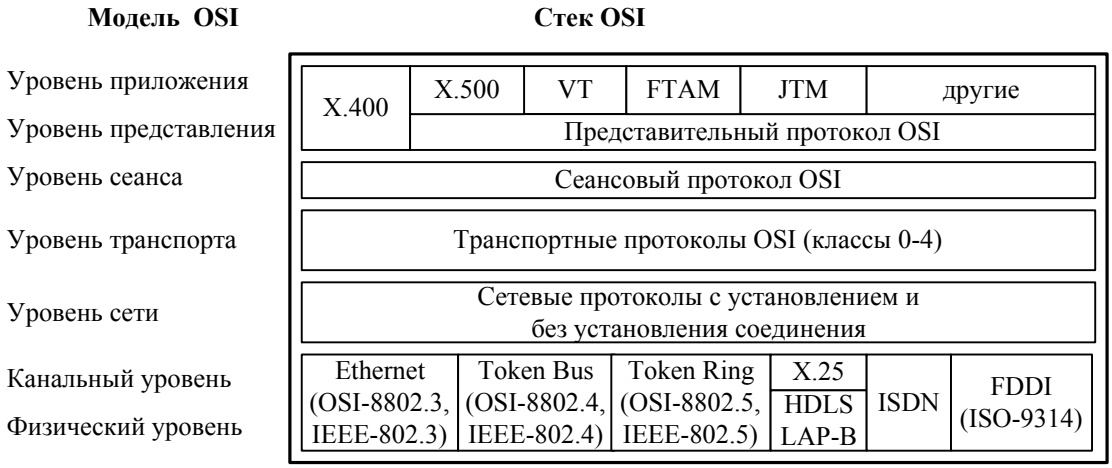

Рис. 2.1. Стек OSI

Сервисы *прикладного уровня* включают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее перспективными являются служба каталогов (стандарт X.500), электронная почта (X.400), протокол виртуального терминала (VT), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM). В последнее время ISO сконцентрировала свои усилия именно на сервисах верхнего уровня.

2.4. Архитектура стека протоколов Microsoft TCP/IP

Набор многоуровневых протоколов, или как называют стек *TCP/IP* (табл. 2.1), предназначен для использования в различных вариантах сетевого окружения. Стек *TCP/IP* с точки зрения системной архитектуры соответствует эталонной модели *OSI* (Open Systems Interconnection – взаимодействие открытых систем) и позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.

Таблица 2.1

Семейство протоколов TCP/IP

Название протокола	Описание протокола
1	2
WinSock	Сетевой программный интерфейс
NetBIOS	Связь с приложениями ОС Windows
TDI	Интерфейс транспортного драйвера (Transport Driver Interface) позволяет создавать компоненты сеансового уровня.
TCP	Протокол управления передачей (Transmission Control Protocol)
UDP	Протокол пользовательских дейтаграмм (User Datagram Protocol)
ARP	Протокол разрешения адресов (Address Resolution Protocol)
RARP	Протокол обратного разрешения адресов (Reverse Address Resolution Protocol)
IP	Протокол Internet (Internet Protocol)
ICMP	Протокол управляющих сообщений Internet (Internet Control Message Protocol)
IGMP	Протокол управления группами Интернета (Internet Group Management Protocol),
NDIS	Интерфейс взаимодействия между драйверами транспортных протоколов
FTP	Протокол пересылки файлов (File Transfer Protocol)
TFTP	Простой протокол пересылки файлов (Trivial File Transfer Protocol)

Реализация TCP/IP фирмы Microsoft соответствует четырехуровневой модели вместо семиуровневой модели, как показано на рис. 2.2. Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

– уровень *Приложения* модели TCP/IP соответствует уровням *Приложения, Представления* и *Сеанса* модели OSI;

– уровень *Транспорта* модели TCP/IP соответствует аналогичному уровню *Транспорта* модели OSI;

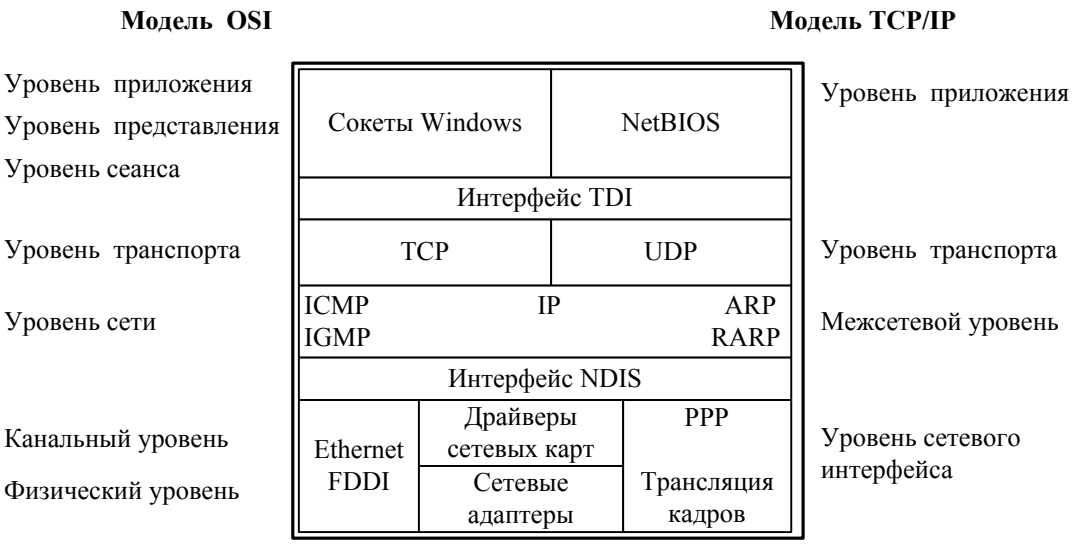

Рис. 2.2. Соответствие семиуровневой модели OSI и четырехуровневой модели TCP/IP

– *межсетевой* уровень модели TCP/IP выполняет те же функции, что и уровень *Сети* модели OSI;

– уровень сетевого интерфейса модели TCP/IP соответствует *Канальному* и *Физическому* уровням модели OSI.

Уровень Приложения

Через уровень *Приложения* модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов (API – Application Programming Interface):

– Сокеты Windows;

– NetBIOS.

Интерфейс *сокетов Windows,* или как его называют *WinSock*, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP – приложениями и семействами протоколов.

Интерфейс *NetBIOS* используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. *NetBIOS* выполняет три основных функции: определение имен NetBIOS; служба дейтаграмм NetBIOS; служба сеанса NetBIOS.

Уровень транспорта

Уровень транспорта TCP/IP отвечает за установления и поддержания соединения между двумя узлами. Основные функции уровня:

– подтверждение получения информации;

– управление потоком данных;

– упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

– TCP (Transmission Control Protocol – протокол управления передачей);

– UDP (User Datagram Protocol – пользовательский протокол дейтаграмм).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные своевременно получены адресатом. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения.

Протокол управления передачей (TCP)

Протокол управления передачей данных – TCP (Transmission Control Protocol) – обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений [6]. Появился в начальный период создания сетей, когда глобальные сети не отличались особой надежностью.

Надежность протокола TCP заключается в следующем:

– он диагностирует ошибки,

– при необходимости посылает данные повторно,

– если не может самостоятельно исправить ошибку, сообщает о ней на другие уровни.

Перед отправкой сегментов информации вниз по модели отправляющий протокол TCP контактирует с принимающим протоколом TCP с целью установления связи. В результате создается *виртуальный канал.* Такой тип коммуникации называется *ориентированным на соединение.*

Установление соединения происходит в три шага:

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также код (определенное число) ISN (Initial Sequence number).

2. Сервер отвечает пакетом, содержащий ISN сервера, а также ISN клиента, увеличенный на 1.

3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенный на 1.

Принцип работы TCP:

– берет из приложения большие блоки информации, разбивает их на сегменты,

– нумерует и упорядочивает каждый сегмент так, чтобы протокол TCP на принимающей стороне мог правильно соединить все сегменты в исходный большой блок;

– согласовывает с протоколом принимающей стороны количество информации, которое должно быть отправлено до получения подтверждения от принимающего TCP;

– после отправки сегментов TCP ждет подтверждения от целевого TCP о получении каждого из них;

– заново отправляет те сегменты, получение которых не было подтверждено.

Трехступенчатое открытие соединения устанавливает номер порта, а также ISN клиента и сервера. Каждый, отправляемый TCP-пакет содержит номера TCP-портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передаче не произошло ошибок. Протокол TCP отвечает за надежную передачу

данных от одного узла сети к другому. Он создает сеанс с установлением соединения, иначе говоря, виртуальный канал между машинами.

Пользовательский протокол дейтаграмм (UDP)

Протокол UDP предназначен для отправки небольших объемов данных (дейтаграмм) без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения [6]. UDP считается более простым протоколом, так как не загромождает сеть служебной информацией и выполняет не все функции TCP. Однако он успешно справляется с передачей информации, не требующей гарантированной доставки, и при этом использует намного меньше сетевых ресурсов. UDP не создает виртуальных каналов и не контактирует с целевым устройством перед отправкой информации. Поэтому он считается протоколом без постоянного соединения, или *не ориентированным на соединение* [3].

Принцип работы UDP:

– получает с верхних уровней блоки информации, разбивает их на сегменты;

– нумерует каждый из сегментов, чтобы все сегменты можно было воссоединить в требуемый блок в пункте назначения, но не упорядочивает сегменты и не заботится о том, в каком порядке они поступят в место назначения,

– отправляет сегменты и «забывает» о них;

– не ждет подтверждений о получении и даже не допускает таких подтверждений и потому считается ненадежным протоколом. Но это не значит, что UDP неэффективен – просто он не относится к надежным протоколам.

UDP также использует номера портов для определения конкретного процесса по указанному IP-адресу. Однако UDP-порты отличаются от TCP-портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами.

Межсетевой уровень

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети). В стеке TCP/IP на этом уровне используется протокол IP.

Протокол Интернета IP

Протокол IP обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую. Данный протокол не ожидает получение подтверждения (ASK, Acknowledgment) отправленных пакетов от узла адресата. Подтверждения, а также повторные отправки пакетов осуществляется протоколами и процессами, работающими на верхних уровнях модели.

К его функциям относится фрагментация дейтаграмм и межсетевая адресация. Протокол IP предоставляет управляющую информацию для сборки фрагментированных дейтаграмм. Главной функцией протокола является межсетевая и глобальная адресация. В зависимости от размера сети, по которой будет маршрутизироваться дейтаграмма или пакет, применяется одна из трех схем адресации.

Адресация в IP-сетях

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя) [3].

Физический, или локальный адрес узла, определяемый технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются

уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Сетевой, или IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла гибкое, и граница между этими полями может устанавливаться произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

При разработке протокола IP на основе размера сетей были выделены их классы (табл. 2.2):

- Класс A – немногочисленные сети с очень большим количеством узлов; номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети.
- Класс B – сети средних размеров; под адрес сети и под адрес узла отводится по 16 битов (по 2 байта).
- Класс C – сети с малым числом узлов; под адрес сети отводится 24 бита (3 байта), а под адрес узла – 8 битов (1 байт).

Таблица 2.2

Классы сетей

Класс	Формат	Диапазон адресов	Максимальное количество сетей	Максимальное количество узлов в одной сети
A	0Сеть.узел.узел.узел	0.0.0.0 – 0.255.255.255	зарезервировано	
		1.0.0.0 – 126.255.255.255	126	16 777 216
		127.0.0.0 – 127.255.255.255	зарезервировано	
B	10Сеть.сеть.узел.узел	128.XXX.0.0 – 191.XXX.255.255	16 384	65 534
C	110Сеть.сеть.сеть.узел	192.XXX.XXX.0 – 223.XXX.255.255	2 097 152	254
D	1110Группа.группа. группа.группа	224.0.0.0 – 239.255.255.255	–	268 435 454
E	1111Резерв.резерв. резерв.резерв	240.0.0.0 – 255.255.255.255	зарезервировано	

- Адреса класса D – особые, групповые адреса – multicast; могут использоваться для рассылки сообщений определенной группе узлов. Если в пакете указан адрес назначения, принадлежащий классу D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Адреса класса E зарезервированы для будущих применений.

Помимо вышеописанных адресов существуют зарезервированные адреса, которые используются особым образом.

• если в поле номера сети стоят 0

0 0 0 0.....0 Номер узла,

то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет: если адрес компьютера 128.187.0.0, то указанный в сообщении адрес 0.0.25.31 неявно преобразуется в адрес 128.187.25.31;

• адрес 127.0.0.X зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной

отправки пакета по сети. Этот адрес имеет название loopback или localhost. Если программа отправит пакет с таким адресом, то этот пакет, не выйдя за пределы компьютера, пройдется по всем уровням сетевой подсистемы и вернется к этой программе. Позволяет разрабатывать и тестировать сетевое программное обеспечение на локальном компьютере, в т. ч. и вообще не имеющем сетевого адаптера.

• если все двоичные разряды IP-адреса равны 1

1 1 1 1.....1 1,

то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и отправитель. Такая рассылка называется *ограниченным широковещательным сообщением* (limited broadcast);

• если в поле адреса узла назначения стоят сплошные 1

Адрес сети 1111.....11,

то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным адресом. Такая рассылка называется *широковещательным сообщением* (broadcast);

• адреса класса D – форма группового IP-адреса – multicast. Пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения, в отличие от широковещательных, называются *мультивещательными.* Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Символьный адрес, или DNS-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес используется на прикладном уровне, например, в протоколах FTP или telnet.

Числовая адресация удобна для машинной обработки таблиц маршрутов. Для использования человеком она представляет

определенные трудности. Для облегчения взаимодействия вначале применялись таблицы соответствия числовых адресов именам машин. Например, в ОС UNIX в каталоге /etc находится файл с именем hosts, который может иметь следующий вид:

IP-адрес Имя машины
127.0.0.1 localhost
144.206.160.32 Polyn
144.206.160.40 Apollo

По мере роста сети была разработана *система доменных имен* – DNS (Domain Name System), которая позволяет присваивать компьютерам легко запоминаемые имена, например yahoo.com, и отвечает за перевод этих имен обратно в IP-адреса. DNS строится по иерархическому принципу, однако, эта иерархия не является строгой. Фактически нет единого корня всех доменов Internet.

Компьютерное имя имеет по меньшей мере два уровня доменов, отделяемых друг от друга точкой (.). Идущие после доменов верхнего уровня домены обычно определяют либо регионы (msk), либо организации (ulstu). Следующие уровни иерархии могут быть закреплены за небольшими организациями, либо за подразделениями больших организаций или частными лицами (например, alvinsoft.h11.ru).

Все, что находится слева, является поддоменом для общего домена. Таким образом, в имени *somesite.uln.ru, somesite* является поддоменом *uln*, который в свою очередь является поддоменом *ru.*

Наиболее популярной программой поддержки DNS является *BIND,* или *Berkeley Internet Name Domain, – сервер доменных имен,* который широко применяется в Internet. Он обеспечивает поиск доменных имен и IP-адресов для любого узла сети. BIND обеспечивает также рассылку сообщений электронной почты через узлы Internet.

BIND реализован по схеме «клиент-сервер». Различают четыре вида серверов:

- *primary master-сервер* поддерживает свою базу данных имен и обслуживает местный домен;

- *secondary master-сервер* обслуживает свой домен, но данные об адресах части своих машин получает по сети с другого сервера;
- *caching-сервер* не имеет своего домена. Он получает данные либо с одного из master-серверов, либо из буфера;
- *удаленный сервер* обычный master-сервер, установленный на удаленной машине, к которому обращаются программы по сети.

Primary или secondary master-серверы устанавливаются обычно на машинах, которые являются шлюзами для локальных сетей.

Шлюз (Gateway) – система, выполняющая преобразование из одного формата в другой.

Сервер имен может быть установлен на любой компьютер локальной сети. При этом необходимо учитывать его производительность, так как многие реализации серверов держат базы данных имен в оперативной памяти. При этом часто подгружается информация и с других серверов. Поэтому это может быть причиной задержек при разрешении запроса на адрес по имени машины.

Протоколы сопоставления адреса ARP и RARP

Для определения локального адреса по IP-адресу используется протокол разрешения адреса *Address Resolution Protocol (ARP)* [3]. ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети – протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), как правило, не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP – *RARP (Reverse Address Resolution Protocol)* и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

В локальных сетях ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.

Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным адресом. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета.

Протокол ICMP

Протокол управления сообщениями Интернета (ICMP – Internet Control Message Protocol) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP-ошибку для уменьшения скорости отправления сообщений. Является частью сетевого уровня набора протоколов TCP/IP.

Протокол ICMP для своих целей использует сообщения, два из которых называются эхо-запрос ICMP и эхо-ответ ICMP:

- Эхо-запрос подразумевает, что компьютер, которому он был отправлен, должен ответить на этот пакет.
- Эхо-ответ – это тип ICMP-сообщения, которое используется для ответа на такой запрос.

Эти сообщения отправляются и принимаются с помощью команды **ping** (Packet Internet Groper).

С помощью специальных пакетов ICMP можно получить информацию:

- о невозможности доставки пакета,
- о превышении времени жизни пакета,
- о превышении продолжительности сборки пакета из фрагментов,
- об аномальных величинах параметров,
- об изменении маршрута пересылки и типа обслуживания,
- о состоянии системы и т. п.

Протокол IGMP

Узлы локальной сети используют протокол управления группами Интернета (IGMP – Internet Group Management Protocol), чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений.

Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

NDIS

Network Device Interface Specification (NDIS) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

Уровень сетевого интерфейса

Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети,

такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

2.5. Контрольные вопросы

1. Назначение спецификации стандартов IEEE802.
2. Какой стандарт описывает сетевую технологию Ethernet?
3. Какой стандарт определяет задачи управления логической связью?
4. Какой стандарт задает механизмы управления сетью?
5. Какой стандарт описывает сетевую технологию ArcNet?
6. Какой стандарт описывает сетевую технологию Token Ring?
7. Какой стандарт содержит рекомендации по оптоволоконным сетевым технологиям?
8. Что такое интерфейс уровня базовой модели OSI?
9. Что такое протокол уровня базовой модели OSI?
10. Дать определение стека протоколов.
11. На какие уровни разбиваются стеки протоколов?
12. Назвать наиболее популярные сетевые протоколы.
13. Назвать наиболее популярные транспортные протоколы.
14. Назвать наиболее популярные прикладные протоколы.
15. Перечислить наиболее популярные стеки протоколов.
16. Назначение программных интерфейсов сокетов Windows и NetBIOS.
17. Чем отличается протокол TCP от UDP?
18. Функции протокола IP.
19. Какие существуют виды адресации в IP-сетях?
20. Какой протокол необходим для определения локального адреса по IP-адресу?
21. Какой протокол необходим для определения IP-адреса по локальному адресу?
22. Какой протокол используется для управления сообщениями Интернета?

3. ТОПОЛОГИЯ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И МЕТОДЫ ДОСТУПА

3.1. Топология вычислительной сети

Топология (конфигурация) – это способ соединения компьютеров в сеть. Тип топологии определяет стоимость, защищенность, производительность и надежность эксплуатации рабочих станций, для которых имеет значение время обращения к файловому серверу.

Понятие топологии широко используется при создании сетей. Одним из подходов к классификации топологий ЛВС является выделение двух основных классов топологий*: широковещательные* и *последовательные*.

В *широковещательных топологиях* ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: *общая шина, дерево, звезда*.

В *последовательных топологиях* информация передается только одному ПК. Примерами таких топологий являются: *произвольная* (произвольное соединение ПК), *кольцо, цепочка*.

При выборе оптимальной топологии преследуются три основных цели:

– обеспечение альтернативной маршрутизации и максимальной надежности передачи данных;

– выбор оптимального маршрута передачи блоков данных;

– предоставление приемлемого времени ответа и нужной пропускной способности.

При выборе конкретного типа сети важно учитывать ее топологию. Основными сетевыми топологиями являются: шинная (линейная) топология, звездообразная, кольцевая и древовидная.

Например, в конфигурации сети ArcNet используется одновременно и линейная, и звездообразная топология. Сети Token Ring физически выглядят как звезда, но логически их пакеты передаются по

кольцу. Передача данных в сети Ethernet происходит по линейной шине, так что все станции видят сигнал одновременно.

Виды топологий

Существуют пять основных топологий (рис. 3.1): общая шина (Bus); кольцо (Ring); звезда (Star); древовидная (Tree); ячеистая (Mesh).

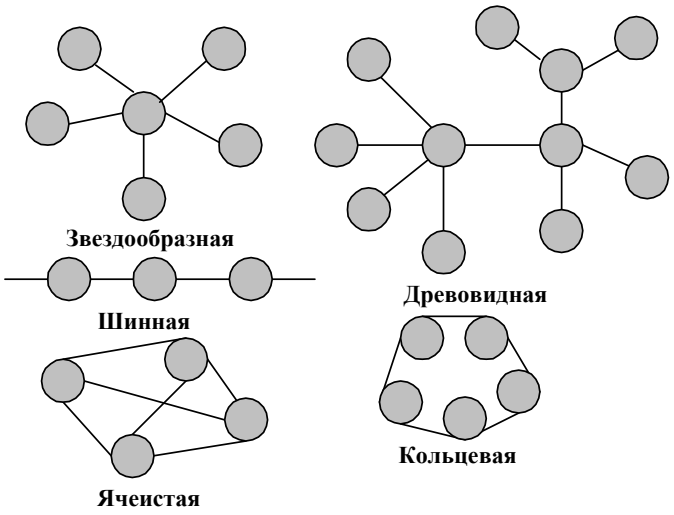

Рис. 3.1. Типы топологий

Общая шина

Общая шина – это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого сегментом. Топология общая шина (рис. 3.2) предполагает использование одного кабеля, к которому подключаются все компьютеры сети.

В случае топологии *Общая шина* кабель используется всеми станциями по очереди:

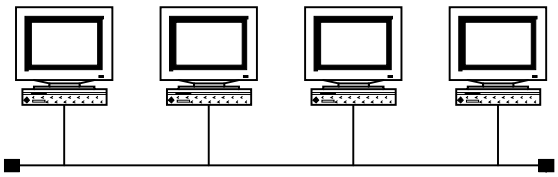

Рис. 3.2. Топология *Общая шина*

1. При передаче пакетов данных каждый компьютер адресует его конкретному компьютеру ЛВС, передавая его по сетевому кабелю в виде электрических сигналов.

2. Пакет в виде электрических сигналов передается по «шине» в обоих направлениях всем компьютерам сети.

3. Однако информацию принимает только тот адрес, который соответствует адресу получателя, указанному в заголовке пакета. Так как в каждый момент времени в сети может вести передачу только одна РС, то производительности ЛВС зависит от количества РС, подключенных к шине. Чем их больше, тем больше ожидающих передачи данных, тем ниже производительности сети. Однако нельзя указать прямую зависимость пропускной способности сети от количества РС, так как на нее также влияют:

- характеристики аппаратного обеспечения РС сети;
- частота, с которой передают сообщения РС;
- тип работающих сетевых приложений;
- тип кабеля и расстояние между РС в сети.

«Шина» – пассивная топология. Это значит, что компьютеры только «слушают» передаваемые по сети данные, но не перемещают их от отправителя к получателю. Поэтому, если один из компьютеров выйдет из строя, это не скажется на работе всей сети.

4. Данные в виде электрических сигналов распространяются по всей сети от одного конца кабеля к другому, и, достигая конца кабеля, будут отражаться и занимать «шину», что не позволит другим компьютерам осуществлять передачу.

5. Чтобы предотвратить отражение электрических сигналов, на каждом конце кабеля устанавливаются терминаторы (Т), поглощающие сигналы, прошедшие по «шине»,

6. При значительном расстоянии между РС (например, 180 м для тонкого коаксиального кабеля) в сегменте «шины» может наблюдаться ослабление электрического сигнала, что может привести к искажению или потере передаваемого пакета данных. В этом случае исходный

сегмент следует разделить на два, установив между ними дополнительное устройство – *репитер (повторитель),* который усиливает принятый сигнал перед тем, как послать его дальше.

Правильно размещенные на длине сети повторители позволяют увеличить длину обслуживаемой сети и расстояние между соседними компьютерами. Следует помнить, что все концы сетевого кабеля должны быть к чему-либо подключены: к РС, терминатору или повторителю.

Разрыв сетевого кабеля или отсоединение одного из его концов приводит к прекращению функционирования сети. Сеть «падает». Сами РС сети остаются полностью работоспособными, но не могут взаимодействовать друг с другом. Если ЛВС на основе сервера, где большая часть программных и информационных ресурсов хранится на сервере, то РС, хотя и остаются работоспособными, но для практической работы малопригодны.

Шинная топология используется в сетях Ethernet, однако в последнее время встречается редко.

Примерами использования топологии общая шина является сеть 10Base-5 (соединение ПК толстым коаксиальным кабелем) и 10Base-2 (соединение ПК тонким коаксиальным кабелем).

Кольцо

Кольцо – это топология ЛВС, в которой каждая станция соединена с двумя другими станциями, образуя кольцо (рис. 3.3). Данные передаются от одной рабочей станции к другой в одном направлении (по кольцу). Каждый ПК работает как повторитель, ретранслируя сообщения к следующему ПК, т.е. данные, передаются от одного компьютера к другому как бы по эстафете. Если компьютер получает данные, предназначенные для другого компьютера, он передает их дальше по кольцу, в ином случае они дальше не передаются. Основная проблема при кольцевой топологии заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации,

и в случае выхода из строя хотя бы одной из них, вся сеть парализуется. Подключение новой рабочей станции требует краткосрочного выключения сети, т.к. во время установки кольцо должно быть разомкнуто. Топология *Кольцо* имеет хорошо предсказуемое время отклика, определяемое числом рабочих станций.

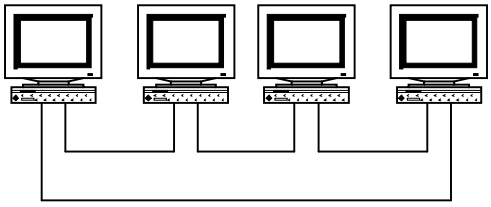

Рис. 3.3. Топология *Кольцо*

Чистая кольцевая топология используется редко. Вместо этого кольцевая топология играет транспортную роль в схеме метода доступа. Кольцо описывает логический маршрут, а пакет передается от одной станции к другой, совершая в итоге полный круг. В сетях Token Ring кабельная ветвь из центрального концентратора называется MAU (Multiple Access Unit). MAU имеет внутреннее кольцо, соединяющее все подключенные к нему станции, и используется как альтернативный путь, когда оборван или отсоединен кабель одной рабочей станции. Когда кабель рабочей станции подсоединен к MAU, он просто образует расширение кольца: сигналы поступают к рабочей станции, а затем возвращаются обратно во внутреннее кольцо.

Звезда

Звезда – это топология ЛВС (рис. 3.4), в которой все *рабочие станции* присоединены к центральному узлу (например, к концентратору), который устанавливает, поддерживает и разрывает связи между рабочими станциями. Преимуществом такой топологии является возможность простого исключения неисправного *узла*. Однако, если неисправен центральный узел, вся сеть выходит из строя.

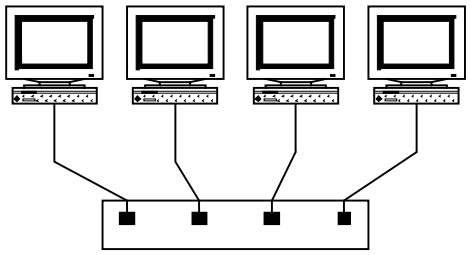

Рис. 3.4. Топология *Звезда*

В этом случае каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству. При необходимости можно объединять вместе несколько сетей с топологией *Звезда,* при этом получаются разветвленные конфигурации сети. В каждой точке ветвления необходимо использовать специальные соединители (распределители, повторители или устройства доступа).

Примером звездообразной топологии является топология Ethernet с кабелем типа *Витая пара* 10BASE-T, центром *Звезды* обычно является Hub.

Звездообразная топология обеспечивает защиту от разрыва кабеля. Если кабель рабочей станции будет поврежден, это не приведет к выходу из строя всего сегмента сети. Она позволяет также легко диагностировать проблемы подключения, так как каждая рабочая станция имеет свой собственный кабельный сегмент, подключенный к концентратору. Для диагностики достаточно найти разрыв кабеля, который ведет к неработающей станции. Остальная часть сети продолжает нормально работать.

Однако звездообразная топология имеет и недостатки. Во-первых, она требует много кабеля. Во-вторых, концентраторы довольно дороги. В-третьих, кабельные концентраторы при большом количестве кабеля трудно обслуживать. Однако в большинстве случаев в такой топологии используется недорогой кабель типа *витая пара*. В некоторых случаях можно даже использовать существующие телефонные кабели. Кроме того, для диагностики и тестирования выгодно собирать все кабельные концы в одном месте.

Сравнительные характеристики базовых сетевых топологий представлены в табл. 3.1.

Таблица 3.1

Сравнительные характеристики базовых сетевых топологий

Топология	Преимущества	Недостатки
1	2	3
«Шина»	- экономный расход кабеля; - недорогая и несложная в использовании среда передачи; - простота и надежность; - легкая расширяемость	- при значительных объемах трафика уменьшается пропускная способность; - трудная локализация проблем; -выход из строя любого сегмента кабеля остановит работу всей сети
«Кольцо»	- все PC имеют равный доступ; - количество пользователей не сказывается на производительности	- выход из строя одной PC выводит из строя всю сеть; - трудно локализовать проблемы; - изменение конфигурации сети требует остановки всей сети
«Звезда»	- легко производить монтаж сети или модифицировать сеть, добавляя новые PC; - централизованный контроль и управление; - выход из строя одного PC или одного сегмента кабеля не влияет на работу всей сети	Выход из строя или отключение питания концентратора (коммутатора) выводит из строя всю сеть; большой расход кабеля

3.2. Методы доступа

Метод доступа – это способ определения того, какая из рабочих станций сможет следующей использовать ЛВС. То, как сеть управляет доступом к каналу связи (кабелю), существенно влияет на ее характеристики. Примерами методов доступа являются:

– множественный доступ с прослушиванием несущей и разрешением коллизий (Carrier Sense Multiple Access with Collision Detection – CSMA/CD);

– множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод с передачей маркера;

– множественный доступ с разделением во времени (Time Division Multiple Access – TDMA);

– множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wavelength Division Multiple Access – WDMA).

CSMA/CD

Метод множественного доступа с прослушиванием несущей и разрешением коллизий (CSMA/CD) устанавливает следующий порядок: если рабочая станция хочет воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала: начинать передачу станция может, если канал свободен. В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата, выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу. Принимающая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообщение, в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

Алгоритм множественного доступа с прослушиванием несущей и разрешением коллизий приведен на рис. 3.5.

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

Рис. 3.5. Алгоритм *CSMA/CD*

Стандарт типа *Ethernet* определяет сеть с конкуренцией, в которой несколько рабочих станций должны конкурировать друг с другом за право доступа к сети.

ТРМА

Метод с передачей маркера – это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция – адресат принимает его. При этом она создает новый маркер.

Маркер (token), или полномочие, – уникальная комбинация битов, позволяющая начать передачу данных.

Алгоритм множественного доступа с передачей полномочия, или маркера, приведен на рис. 3.6.

Рис. 3.6. Алгоритм TPMA

Каждый узел принимает пакет от предыдущего, восстанавливает уровни сигналов до номинального уровня и передает дальше. Передаваемый пакет может содержать данные или являться маркером. Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет,

содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по ЛВС.

Пакет распространяется по ЛВС от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в ЛВС. После чего пакет возвращается в узел из которого был отправлен. Здесь после проверки безошибочной передачи пакета, узел освобождает ЛВС, выпуская новый маркер.

Таким образом, в ЛВС с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

– гарантирует определенное время доставки блоков данных в сети;

– дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

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

– включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

TDMA

Множественный доступ с разделением во времени основан на распределении времени работы канала между системами (рис. 3.7).

Доступ *TDMA* основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается сигналом *Разграничителем*. Цикл включает *n* пронумерованных временных интервалов, называемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.

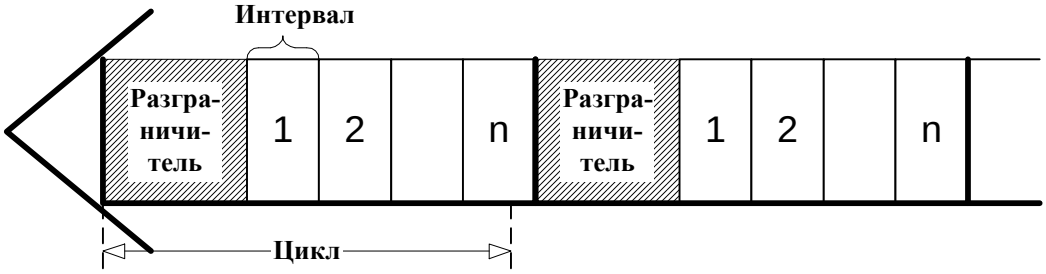

Рис. 3.7. Структура множественного доступа с разделением во времени

Данный способ позволяет организовать передачу данных с коммутацией пакетов и с коммутацией каналов.

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

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

FDMA

Доступ *FDMA* основан на разделении полосы пропускания канала на группу полос частот (рис. 3.8), образующих *логические каналы*.

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

При использовании FDMA, именуемого также *множественным доступом с разделением волны* WDMA, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале.

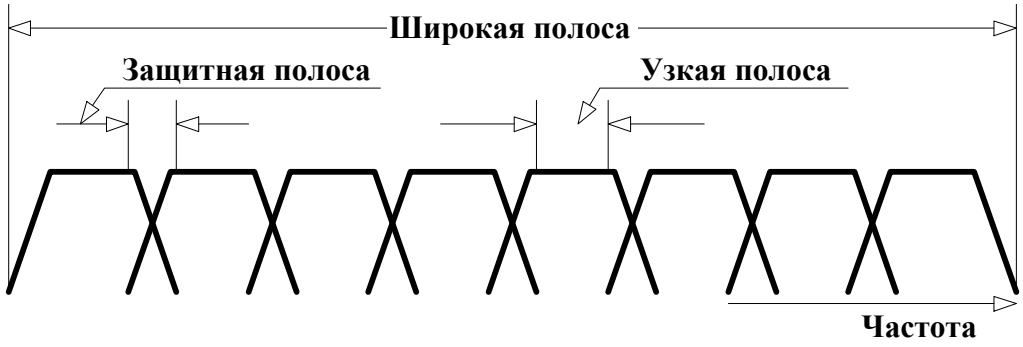

Рис. 3.8. Схема выделения логических каналов

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

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

3.3. Технологии локальных сетей

Технология Ethernet

Ethernet – это самый распространенный на сегодняшний день стандарт локальных сетей [3].

Ethernet – это сетевой стандарт, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году.

В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля, который стал последней версией фирменного стандарта Ethernet. Поэтому фирменную версию стандарта Ethernet называют *стандартом* Ethernet DIX, или Ethernet II, на основе которых был разработан стандарт *IEEE 802.3.*

На основе стандарта Ethernet были приняты дополнительные стандарты: в 1995 году Fast Ethernet (дополнение к *IEEE 802.3*), в 1998 году Gigabit Ethernet (раздел IEEE 802.3z основного документа), которые во многом не являются самостоятельными стандартами.

Для передачи двоичной информации по кабелю для всех вариантов физического уровня технологии Ethernet, обеспечивающих пропускную способность 10 Мбит/с, используется манчестерский код (рис. 3.9).

В манчестерском коде для кодирования единиц и нулей используется перепад потенциала, то есть фронт импульса. При манчестерском кодировании каждый такт делится на две части. Информация кодируется перепадами потенциала, происходящими в середине каждого такта. Единица кодируется перепадом от низкого уровня сигнала к высокому (передним фронтом импульса), а ноль – обратным перепадом (задним фронтом).

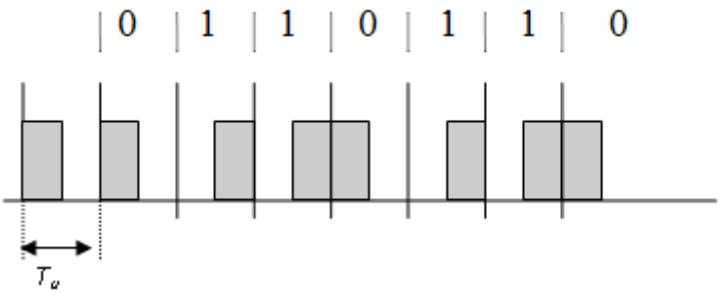

Рис. 3.9. Дифференциальное манчестерское кодирование

В стандарте Ethernet (в том числе Fast Ethernet и Gigabit Ethernet) используется один и тот же метод разделения среды передачи данных – метод CSMA/CD.

Каждый ПК работает в Ethernet согласно принципу «Слушай канал передачи, перед тем как отправить сообщения; слушай, когда отправляешь; прекрати работу в случае помех и попытайся еще раз».

Данный принцип можно расшифровать (объяснить) следующим образом:

1. Никому не разрешается посылать сообщения в то время, когда этим занят уже кто-то другой (слушай перед тем, как отправить).
2. Если два или несколько отправителей начинают посылать сообщения примерно в один и тот же момент, рано или поздно их сообщения «столкнутся» друг с другом в канале связи, что называется *коллизией*.

Коллизии нетрудно распознать, поскольку они всегда вызывают сигнал помехи, который не похож на допустимое сообщение. Ethernet может распознать помехи и заставляет отправителя приостановить передачу и подождать некоторое время, прежде, чем повторно отправить сообщение.

Причины широкой распространенности и популярности Ethernet (достоинства):

1. Дешевизна.
2. Большой опыт использования.
3. Продолжающиеся нововведения.

4. Богатство выбора оборудования. Многие изготовители предлагают аппаратуру построения сетей, базирующуюся на Ethernet.

Недостатки Ethernet:

1. Возможность столкновений сообщений (коллизии, помехи).
2. В случае большой загрузки сети время передачи сообщений непредсказуемо.

Технология Token Ring

Сети Token Ring, как и сети Ethernet, характеризует *разделяемая среда передачи данных*, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо [5]. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему требуется не случайный алгоритм, как в сетях Ethernet, а детерминированный, основанный на передаче станциям права на использование кольца в определенном порядке. Это право передается с помощью кадра специального формата, называемого *маркером,* или *токеном (token)* [3].

Технология Token Ring был разработана компанией IBM в 1984 году, а затем передана в качестве проекта стандарта в комитет IEEE 802, который на ее основе принял в 1985 году стандарт 802.5.

Каждый ПК работает в Token Ring согласно принципу «Ждать маркера, если необходимо послать сообщение, присоединить его к маркеру, когда он будет проходить мимо. Если проходит маркер, снять с него сообщение и отправить маркер дальше».

Сети Token Ring работают с двумя битовыми скоростями – 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается.

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры – посланный кадр всегда возвращается в станцию-отправитель.

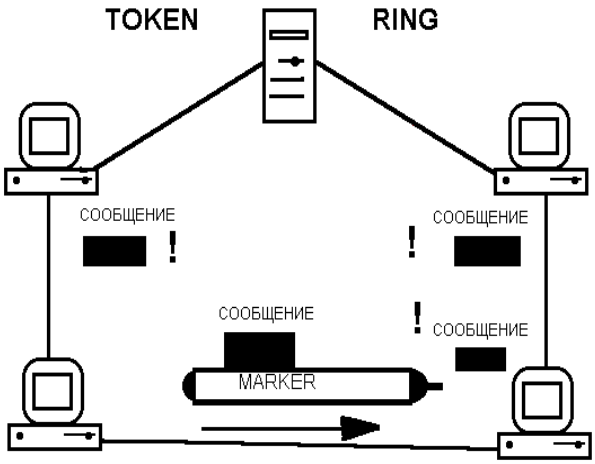

Рис. 3.10. Принцип технологии TOKEN RING

В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например, может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

Для контроля сети одна из станций выполняет роль так называемого *активного монитора.* Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC-адреса. Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Сеть Token Ring может включать до 260 узлов.

Концентратор Token Ring может быть активным или пассивным. Пассивный концентратор просто соединяет порты внутренними связями так, чтобы станции, подключаемые к этим портам, образовали кольцо. Ни усиление сигналов, ни их ресинхронизацию пассивный MSAU не выполняет.

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

В общем случае сеть Token Ring имеет комбинированную звездно-кольцевую конфигурацию. Конечные узлы подключаются к MSAU по топологии звезды, а сами MSAU объединяются через специальные порты Ring In (RI) и Ring Out (RO) для образования магистрального физического кольца.

Все станции в кольце должны работать на одной скорости либо 4 Мбит/с, либо 16 Мбит/с. Кабели, соединяющие станцию с концентратором, называются *ответвительными* (lobe cable), а кабели, соединяющие концентраторы, – *магистральными* (trunk cable).

Технология Token Ring позволяет использовать для соединения конечных станций и концентраторов различные типы кабеля:

– STP Type 1 – экранированная витая пара (Shielded Twistedpair). В кольцо допускается объединять до 260 станций при длине ответвительных кабелей до 100 метров;

– UTP Type 3, UTP Type 6 – неэкранированная витая пара (Unshielded Twistedpair). Максимальное количество станций сокращается до 72 при длине ответвительных кабелей до 45 метров;

– волоконно-оптический кабель.

Расстояние между пассивными MSAU может достигать 100 м при использовании кабеля STP Type 1 и 45 м при использовании кабеля UTP Type 3. Между активными MSAU максимальное расстояние увеличивается соответственно до 730 м или 365 м в зависимости от типа кабеля.

Максимальная длина кольца Token Ring составляет 4000 м. Ограничения на максимальную длину кольца и количество станций в кольце в технологии Token Ring не являются такими жесткими, как в технологии Ethernet. Здесь эти ограничения в основном связаны со временем оборота маркера по кольцу.

Все значения тайм-аутов в сетевых адаптерах узлов сети Token Ring можно настраивать, поэтому можно построить сеть Token Ring с большим количеством станций и с большей длиной кольца.

Преимущества технологии Token Ring:

- гарантированная доставка сообщений;
- высокая скорость передачи данных (до 160% Ethernet).

Недостатки технологии Token Ring:

- необходимы дорогостоящие устройства доступа к среде;
- технология более сложная в реализации;

- необходимы 2 кабеля (для повышения надежности): один входящий, другой исходящий от компьютера к концентратору;
- высокая стоимость (160-200% от Ethernet).

Технология FDDI

Технология *FDDI (Fiber Distributed Data Interface)* – оптоволоконный интерфейс распределенных данных – это первая технология локальных сетей, в которой средой передачи данных является волоконно-оптический кабель. Технология появилась в середине 80-х годов [5].

Технология FDDI во многом основывается на технологии Token Ring, поддерживая метод доступа с передачей маркера.

Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Наличие двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят воспользоваться этим повышенным потенциалом надежности, должны быть подключены к обоим кольцам.

В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля только первичного (Primary) кольца, этот режим назван режимом *Thru* – «сквозным», или «транзитным». Вторичное кольцо (Secondary) в этом режиме не используется.

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется с вторичным, вновь образуя единое кольцо. Этот режим работы сети называется *Wrap,* то есть «свертывание» или «сворачивание» колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров FDDI.

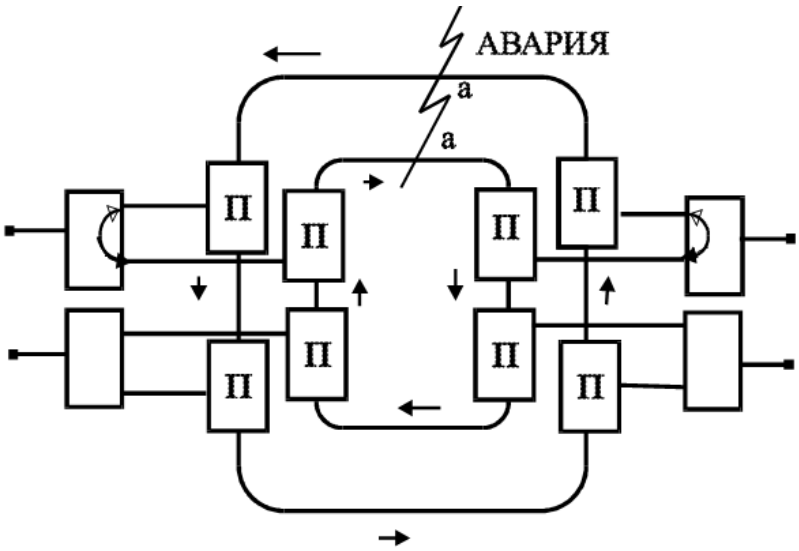

Рис. 3.11. ИВС с двумя циклическими кольцами в аварийном режиме

Для упрощения этой процедуры данные по первичному кольцу всегда передаются в одном направлении (на диаграммах это направление изображается против часовой стрелки), а по вторичному – в обратном (изображается по часовой стрелке). Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

Сеть FDDI может полностью восстанавливать свою работоспособность в случае единичных отказов ее элементов. При множественных отказах сеть распадается на несколько не связанных сетей.

Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа сетей Token Ring и также называется *методом маркерного* (или токенного) *кольца* – token ring.

Отличия метода доступа заключаются в том, что время удержания маркера в сети FDDI не является постоянной величиной. Это время зависит от загрузки кольца – при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшаться до нуля.

Эти изменения в методе доступа касаются только асинхронного трафика, который не критичен к небольшим задержкам передачи кадров. Для синхронного трафика время удержания маркера по-прежнему остается фиксированной величиной.

Технология FDDI в настоящее время поддерживает типа кабелей:

– волоконно-оптический кабель;

– неэкранированная витая пара категории 5. Последний стандарт появился позже оптического и носит название TP-PMD (Physical Media Dependent).

Оптоволоконная технология обеспечивает необходимые средства для передачи данных от одной станции к другой по оптическому волокну и определяет:

• использование в качестве основной физической среды многомодового волоконно-оптического кабеля 62,5/125 мкм;

• требования к мощности оптических сигналов и максимальному затуханию между узлами сети. Для стандартного многомодового кабеля эти требования приводят к предельному расстоянию между узлами в 2 км, а для одномодового кабеля расстояние увеличивается до 10–40 км в зависимости от качества кабеля;

• требования к оптическим обходным переключателям (optical bypass switches) и оптическим приемопередатчикам;

• параметры оптических разъемов MIC (Media Interface Connector), их маркировку;

• использование для передачи света с длиной волны в 1,3 нм;

Максимальная общая длина кольца FDDI составляет 100 километров, максимальное число станций с двойным подключением в кольце – 500.

Технология FDDI разрабатывалась для применения в ответственных участках сетей – на магистральных соединениях между крупными сетями, например сетями зданий, а также для подключения к сети высокопроизводительных серверов. Поэтому главные требования, у разработчиков были (**достоинства**):

- обеспечение высокой скорости передачи данных,

- отказоустойчивость на уровне протокола;

- большие расстояния между узлами сети и большое количество подключенных станций.

Все эти цели были достигнуты. В результате технология FDDI получилась качественной, но весьма дорогой (**недостаток**). Даже появление более дешевого варианта для витой пары не намного снизило стоимость подключения одного узла к сети FDDI. Поэтому практика показала, что основной областью применения технологии FDDI стали магистрали сетей, состоящих из нескольких зданий, а также сети масштаба крупного города, то есть класса MAN.

Технология Fast Ethernet

Потребности в высокоскоростной и в то же время недорогой технологии для подключения к сети мощных рабочих станций привели в начале 90-х годов к созданию инициативной группы, которая занялась поисками нового Ethernet, такой же простой и эффективной технологии, но работающей на скорости 100 Мбит/с [5].

Специалисты разбились на два лагеря, что в конце концов привело к появлению двух стандартов, принятых осенью 1995 года: комитет 802.3 утвердил стандарт Fast Ethernet, почти полностью повторяющий технологию Ethernet 10 Мбит/с.

Технология Fast Ethernet сохранила в неприкосновенности метод доступа CSMA/CD, оставив в нем тот же алгоритм и те же временные параметры в битовых интервалах (сам битовый интервал уменьшился в 10 раз). Все отличия Fast Ethernet от Ethernet проявляются на физическом уровне.

В стандарте Fast Ethernet определены три спецификации физического уровня:

- 100Base-TX для 2-х пар UTP категории 5 или 2-х пар STP Type 1 (метод кодирования 4B/5B);

- l00Base-FX для многомодового волоконно-оптического кабеля с двумя оптическими волокнами (метод кодирования 4B/5B);

- 100Base-T4, работающую на 4-х парах UTP категории 3, но использующую одновременно только три пары для передачи, а оставшуюся – для обнаружения коллизии (метод кодирования 8B/6T).

Стандарты l00Base-TX/FX могут работать в полнодуплексном режиме.

Максимальный диаметр сети Fast Ethernet равен приблизительно 200 м, а более точные значения зависят от спецификации физической среды. В домене коллизий Fast Ethernet допускается не более одного повторителя класса I (позволяющего транслировать коды 4B/5B в коды 8B/6T и обратно) и не более двух повторителей класса II (не позволяющих выполнять трансляцию кодов).

Технология Fast Ethernet при работе на витой паре позволяет за счет процедуры автопереговоров двум портам выбирать наиболее эффективный режим работы – скорость 10 Мбит/с или 100 Мбит/с, а также полудуплексный или полнодуплексный режим.

Технология Gigabit Ethernet

Технология Gigabit Ethernet добавляет новую, 1000 Мбит/с, ступень в иерархии скоростей семейства Ethernet. Эта ступень позволяет эффективно строить крупные локальные сети, в которых мощные серверы и магистрали нижних уровней сети работают на скорости 100 Мбит/с, а магистраль Gigabit Ethernet объединяет их, обеспечивая достаточно большой запас пропускной способности.

Разработчики технологии Gigabit Ethernet сохранили большую степень преемственности с технологиями Ethernet и Fast Ethernet. Gigabit Ethernet использует те же форматы кадров, что и предыдущие версии Ethernet, работает в полнодуплексном и полудуплексном режимах, поддерживая на разделяемой среде тот же метод доступа CSMA/CD с минимальными изменениями.

Для обеспечения приемлемого максимального диаметра сети в 200 м в полудуплексном режиме разработчики технологии пошли на увеличение минимального размера кадра в 8 раз (с 64 до 512 байт). Разрешается также передавать несколько кадров подряд, не освобождая среду, на интервале 8096 байт, тогда кадры не обязательно дополнять до 512 байт. Остальные параметры метода доступа и максимального размера кадра остались неизменными.

Летом 1998 года был принят стандарт 802.3z, который определяет использование в качестве физической среды трех типов кабеля:

- многомодового оптоволоконного (расстояние до 500 м),
- одномодового оптоволоконного (расстояние до 5000 м),
- двойного коаксиального (twinax), по которому данные передаются одновременно по двум медным экранированным проводникам на расстояние до 25 м.

Для разработки варианта Gigabit Ethernet на UTP категории 5 была создана специальная группа 802.3ab, которая уже разработала проект стандарта для работы по 4-м парам UTP категории 5. Принятие этого стандарта ожидается в ближайшее время.

3.4. Контрольные вопросы

1. Что такое топология?
2. Перечислить наиболее используемые типы топологий?
3. Охарактеризовать топологию *Общая шина* и привести примеры использования данной топологии.
4. Какие сетевые технологии используют топологию *Общая шина*?
5. Охарактеризовать топологию *Кольцо* и привести примеры этой топологии.
6. В каких случаях используют топологию *Кольцо*?
7. Охарактеризовать топологию *Звезда* и привести примеры использования этой топологии.
8. К какой топологии относится сеть при подсоединении всех компьютеров к общему концентратору?

9. Привести примеры и охарактеризовать древовидную топологию.
10. Что такое ячеистая топология и в каких случаях она используется?
11. Что такое метод доступа и как влияет метод доступа на передачу данных в сети?
12. Какие существуют методы доступа?
13. Охарактеризовать метод доступа с прослушиванием несущей и разрешением коллизий.
14. При каком методе доступа обе станции могут одновременно начать передачу и войти в конфликт?
15. В каких сетевых технологиях используется метод *CSMA/CD*?
16. Охарактеризовать метод доступа с разделением во времени и перечислить в каких случаях используется данный метод.
17. Что такое маркер?
18. В каком случае рабочая станция может начать передачу данных при использовании метода доступа с передачей полномочия?
19. Охарактеризовать метод доступа с передачей полномочия.
20. Охарактеризовать метод множественного доступа с разделением частоты.
21. Какие существуют варианты использования множественного доступа с разделением во времени?

4. ЛВС И КОМПОНЕНТЫ ЛВС

Компьютерная сеть состоит из трех основных аппаратных компонент и двух программных, которые должны работать согласованно. Для корректной работы устройств в сети их нужно правильно инсталлировать и установить рабочие параметры.

4.1. Основные компоненты

Основными аппаратными компонентами сети являются следующие:

1. Абонентские системы: компьютеры (рабочие станции или клиенты и серверы); принтеры; сканеры и др.

2. Сетевое оборудование: сетевые адаптеры; концентраторы (хабы); мосты; маршрутизаторы и др.

3. Коммуникационные каналы: кабели; разъемы; устройства передачи и приема данных в беспроводных технологиях.

Основными программными компонентами сети являются следующие:

1. Сетевые операционные системы, где наиболее известные из них это: MS Windows; LANtastic; NetWare; Unix; Linux и т.д.

2. Сетевое программное обеспечение (Сетевые службы): клиент сети; сетевая карта; протокол; служба удаленного доступа.

ЛВС (Локальная вычислительная сеть) – это совокупность компьютеров, каналов связи, сетевых адаптеров, работающих под управлением сетевой операционной системы и сетевого программного обеспечения.

В *ЛВС* каждый *ПК* называется *рабочей станцией*, за исключением одного или нескольких компьютеров, которые предназначены для выполнения функций *серверов.* Каждая *рабочая станция* и *сервер* имеют *сетевые карты (адаптеры)*, которые посредством *физических каналов* соединяются между собой. В дополнение к локальной

операционной системе на каждой рабочей станции активизируется сетевое программное обеспечение, позволяющее станции взаимодействовать с файловым сервером.

Компьютеры, входящие в ЛВС клиент – серверной архитектуры, делятся на два типа: *рабочие станции, или клиенты*, предназначенные для пользователей, и *серверы*, которые, как правило, недоступны для обычных пользователей и предназначены для управления ресурсами сети.

Рабочие станции

Рабочая станция (workstation) – это абонентская система, специализированная для решения определенных задач и использующая сетевые ресурсы. К сетевому программному обеспечению рабочей станции относятся следующие службы:

- клиент для сетей;
- служба доступа к файлам и принтерам;
- сетевые протоколы для данного типа сетей;
- сетевая плата;
- контроллер удаленного доступа.

Рабочая станция отличается от обычного автономного персонального компьютера следующим:

- наличием сетевой карты (сетевого адаптера) и канала связи;
- на экране во время загрузки ОС появляются дополнительные сообщения, которые информируют о том, что загружается сетевая операционная система;
- перед началом работы необходимо сообщить сетевому программному обеспечению имя пользователя и пароль. Это называется процедурой входа в сеть;
- после подключения к ЛВС появляются дополнительные сетевые дисковые накопители;

появляется возможность использования сетевого оборудования, которое может находиться далеко от рабочего места.

Сетевые адаптеры

Для подключения *ПК* к сети требуется устройство сопряжения, которое называют сетевым адаптером, интерфейсом, модулем, или картой. Оно вставляется в гнездо материнской платы. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос через сетевой адаптер к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов.

Сетевые адаптеры вместе с сетевым программным обеспечением способны распознавать и обрабатывать ошибки, которые могут возникнуть из-за электрических помех, коллизий или плохой работы оборудования.

Различные типы сетевых адаптеров отличаются не только методами доступа к каналу связи и протоколами, но еще и следующими параметрами:

- скорость передачи;
- объем буфера для пакета;
- тип шины;
- быстродействие шины;
- совместимость с различными микропроцессорами;
- использованием прямого доступа к памяти (DMA);
- адресация портов ввода/вывода и запросов прерывания;

конструкция разъема.

Сетевые операционные системы

Сетевые операционные системы NOS **(**Network Operating System) – это комплекс программ, обеспечивающих в сети обработку, хранение и передачу данных.

Для организации сети кроме аппаратных средств, необходима также сетевая операционная система. Операционные системы сами по себе не могут поддерживать сеть. Для дополнения какой-нибудь ОС сетевыми средствами необходима процедура инсталляции сети.

NOS необходима для управления потоками сообщений между рабочими станциями и файловым сервером. Она является прикладной платформой, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, реализуемых в сетях. NOS используют архитектуру клиент-сервер или одноранговую архитектуру.

NOS определяет группу протоколов, обеспечивающих основные функции сети. К ним относятся:

- адресация объектов сети;
- функционирование сетевых служб;
- обеспечение безопасности данных;
- управление сетью.

Типовой состав оборудования локальной сети

На рис. 4.1 приведен фрагмент вычислительной сети. Фрагмент вычислительной сети включает основные типы коммуникационного оборудования, применяемого сегодня для образования локальных сетей и соединения их через глобальные связи друг с другом.

Для построения локальных связей между компьютерами используются различные виды кабельных систем, сетевые адаптеры, концентраторы, повторители. Для связей между сегментами локальной вычислительной сети используются концентраторы, мосты, коммутаторы, маршрутизаторы и шлюзы.

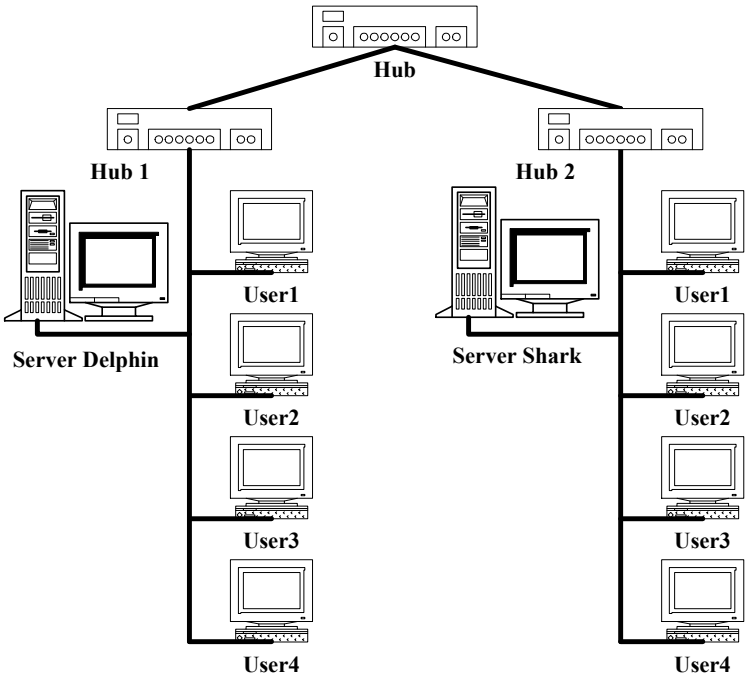

Рис. 4.1. Фрагмент сети

Для подключения локальных сетей к глобальным связям используются:

– специальные выходы (WAN–порты) мостов и маршрутизаторов;

– аппаратура передачи данных по длинным линиям – модемы (при работе по аналоговым линиям);

– устройства подключения к цифровым каналам (ТА – терминальные адаптеры сетей ISDN, устройства обслуживания цифровых выделенных каналов типа CSU/DSU и т.п.).

4.2. Физическая среда передачи данных

Физическая среда является основой, на которой строятся физические средства соединения. Сопряжение с *физическими средствами соединения* посредством физической среды обеспечивает *Физический уровень*. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц. На физическом уровне находится носитель, по которому передаются

данные. Среда передачи данных может включать как кабельные, так и беспроводные технологии. Хотя физические кабели являются наиболее распространенными носителями для сетевых коммуникаций, беспроводные технологии все более внедряются благодаря их способности связывать глобальные сети.

На физическом уровне для физических кабелей определяются механические и электрические (оптические) свойства среды передачи, которые включают:

- тип кабелей и разъемов;
- разводку контактов в разъемах;
- схему кодирования сигналов для значений 0 и 1.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

Кабели связи, линии связи, каналы связи

Для организации связи в сетях используются следующие понятия:

- кабели связи;
- линии связи;
- каналы связи.

Из кабелей связи и других элементов (монтаж, крепеж, кожухи и т.д.) строят *линии связи*. Прокладка линии внутри здания задача достаточно серьезная. Длина линий связи колеблется от десятков метров до десятков тысяч километров. В любую более-менее серьезную линию связи кроме кабелей входят: траншеи, колодцы, муфты, переходы через реки, море и океаны, а также грозозащита (равно как и другие виды защиты) линий. Очень сложны охрана, эксплуатация, ремонт линий связи; содержание кабелей связи под избыточным давлением, профилактика (в снег, дождь, на ветру, в траншее и в

колодце, в реке и на дне моря). Большую сложность представляют собой юридические вопросы, включающие согласование прокладки линий связи, особенно в городе. Вот чем линия (связи) отличается от кабеля.

По уже построенным линиям организуют *каналы связи*. Причем если линию, как правило, строят и сдают сразу всю, то каналы связи вводят постепенно. Уже по линии можно дать связь, но такое использование крайне дорогостоящих сооружений очень неэффективно. Поэтому применяют аппаратуру каналообразования (или, как раньше говорили, уплотнение линии). По каждой электрической цепи, состоящей из двух проводов, обеспечивают связь не одной паре абонентов (или компьютеров), а сотням или тысячам: по одной коаксиальной паре в междугородном кабеле может быть образовано до 10800 каналов тональной частоты (0,3–3,4 КГц) или почти столько же цифровых, с пропускной способностью 64 Кбит/с.

При наличии кабелей связи создаются линии связи, а уже по линиям связи создаются каналы связи. Линии связи и каналы связи заводятся на узлы связи. Линии, каналы и узлы образуют первичные сети связи.

Типы кабелей и структурированные кабельные системы

В качестве среды передачи данных используются различные виды кабелей: коаксиальный кабель, кабель на основе экранированной и неэкранированной витой пары и оптоволоконный кабель. Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) становится *неэкранированная витая пара*, которая включена практически во все современные стандарты и технологии локальных сетей и обеспечивает пропускную способность до 100 Мб/с (на кабелях категории 5). *Оптоволоконный кабель* широко применяется как для построения локальных связей, так и для образования магистралей глобальных сетей. Оптоволоконный кабель может обеспечить очень высокую пропускную способность канала (до нескольких Гб/с) и

передачу на значительные расстояния (до нескольких десятков километров без промежуточного усиления сигнала).

В качестве среды передачи данных в вычислительных сетях используются также электромагнитные волны различных. Однако пока в локальных сетях радиосвязь используется только в тех случаях, когда оказывается невозможной прокладка кабеля, например, в зданиях. Это объясняется недостаточной надежностью сетевых технологий, построенных на использовании электромагнитного излучения. Для построения глобальных каналов этот вид среды передачи данных используется шире – на нем построены спутниковые каналы связи и наземные радиорелейные каналы, работающие в зонах прямой видимости в СВЧ диапазонах.

Очень важно правильно построить фундамент сети – кабельную систему. В последнее время в качестве такой надежной основы все чаще используется *структурированная кабельная система*.

Структурированная кабельная система SCS (Structured Cabling System) – это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Преимущества структурированной кабельной системы.

– *Универсальность.* Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети.

– *Увеличение срока службы.* Срок старения хорошо структурированной кабельной системы может составлять 8-10 лет.

– *Уменьшение стоимости добавления новых пользователей и изменения их мест размещения.* Стоимость кабельной системы в основном определяется не стоимостью кабеля, а стоимостью работ по его прокладке.

– *Возможность легкого расширения сети.* Структурированная кабельная система является модульной, поэтому ее легко наращивать,

позволяя легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.

– *Обеспечение более эффективного обслуживания.* Структурированная кабельная система облегчает обслуживание и поиск неисправностей.

– *Надежность.* Структурированная кабельная система имеет повышенную надежность, поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.

Существует несколько различных типов кабелей, используемых в современных сетях. Ниже приведены наиболее часто используемые типы кабелей. Множество разновидностей медных кабелей составляют класс электрических кабелей, используемых как для прокладки телефонных сетей, так и для инсталляции ЛВС. По внутреннему строению различают кабели на витой паре и коаксиальные кабели.

Кабель типа «витая пара» (twisted pair)

Витой парой называется кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю, а *экранированные витые пары* еще более увеличивают степень помехозащищенности сигналов.

Кабель типа «витая пара» используется во многих сетевых технологиях, включая Ethernet, ARCNet и IBM Token Ring.

Кабели на витой паре подразделяются на: неэкранированные UTP (Unshielded Twisted Pair) и экранированные медные кабели. Последние подразделяются на две разновидности: с экранированием каждой пары и общим экраном STP (Shielded Twisted Pair) и с одним только общим экраном FTP (Foiled Twisted Pair). Наличие или отсутствие экрана у кабеля вовсе не означает наличия или отсутствия защиты передаваемых данных, а говорит лишь о различных подходах к подавлению помех.

Отсутствие экрана делает неэкранированные кабели более гибкими и устойчивыми к изломам. Кроме того, они не требуют дорогостоящего контура заземления для эксплуатации в нормальном режиме, как экранированные. Неэкранированные кабели идеально подходят для прокладки в помещениях внутри офисов, а экранированные лучше использовать для установки в местах с особыми условиями эксплуатации, например, рядом с очень сильными источниками электромагнитных излучений, которых в офисах обычно нет.

Кабели классифицируются по категориям, указанным в табл. 4.1. Основанием для отнесения кабеля к одной из категорий служит максимальная частота передаваемого по нему сигнала.

Таблица 4.1

Категории кабелей

Категория	Частота передаваемого сигнала, (МГц)
3	16
4	20
5	100
5+	300
6	200
7	600

Коаксиальные кабели

Коаксиальные кабели используются в радио и телевизионной аппаратуре. *Коаксиальные кабели* могут передавать данные со скоростью 10 Мбит/с на максимальное расстояние от 185 до 500 метров. Они разделяются на *толстые* и *тонкие* в зависимости от толщины. Типы коаксиальных кабелей приведены в табл. 4.2.

Кабель Thinnet, известный как кабель RG-58, является наиболее широко используемым физическим носителем данных. Сети при этом не требуют дополнительного оборудования и являются простыми и недорогими. Хотя *тонкий коаксиальный кабель (Thin Ethernet)* позволяет передачу на меньшее расстояние, чем толстый, но для

соединений *с тонким кабелем* применяются стандартные байонетные разъемы *BNC* типа *CP-50* и ввиду его небольшой стоимости он становится фактически стандартным для офисных ЛВС. Используется в технологии *Ethernet 10Base2*.

Таблица 4.2

Типы коаксиальных кабелей

Тип	Название, значение сопротивления
RG-8 и RG-11	Thicknet, 50 Ом
RG-58/U	Thinnet, 50 Ом, сплошной центральный медный проводник
RG-58 A/U	Thinnet, 50 Ом, центральный многожильный проводник
RG-59	Broadband/Cable television (широковещательное и кабельное телевидение), 75 Ом
RG-59 /U	Broadband/Cable television (широковещательное и кабельное телевидение), 50 Ом
RG-62	ARCNet, 93 Ом

Толстый коаксиальный кабель (Thick Ethernet) имеет большую степень помехозащищенности, большую механическую прочность, но требует специального приспособления для прокалывания кабеля, чтобы создать ответвления для подключения к ЛВС. Он более дорогой и менее гибкий, чем тонкий. Используется в технологии *Ethernet 10Base5*, описанной ниже. Сети ARCNet с посылкой маркера обычно используют кабель RG-62 A/U.

Оптоволоконный кабель

Отличительная особенность оптоволоконных систем – высокая стоимость как самого кабеля (по сравнению с медным), так и специализированных установочных элементов (розеток, разъемов, соединителей и т. п.). Правда, главный вклад в стоимость сети вносит цена активного сетевого оборудования для оптоволоконных сетей.

Оптоволоконные сети применяются для горизонтальных высокоскоростных каналов, а также все чаще стали применяться для вертикальных каналов связи (межэтажных соединений).

Оптоволоконный кабель (Fiber Optic Cable) обеспечивает высокую скорость передачи данных на большом расстоянии. Они также невосприимчивы к интерференции и подслушиванию. В *оптоволоконном кабеле* для передачи сигналов используется свет. Волокно, применяемое в качестве световода, позволяет передачу сигналов на большие расстояния с огромной скоростью, но оно дорого, и с ним трудно работать.

Для установки разъемов, создания ответвлений, поиска неисправностей в *оптоволоконном кабеле* необходимы специальные приспособления и высокая квалификация. *Оптоволоконный кабель* состоит из центральной стеклянной нити толщиной в несколько микрон, покрытой сплошной стеклянной оболочкой. Все это, в свою очередь, спрятано во внешнюю защитную оболочку.

Оптоволоконные линии очень чувствительны к плохим соединениям в разъемах. В качестве источника света в таких кабелях применяются *светодиоды*, а информация кодируется путем изменения интенсивности света. На приемном конце кабеля детектор преобразует световые импульсы в электрические сигналы.

Существуют два типа оптоволоконных кабелей – одномодовые и многомодовые. Одномодовые кабели имеют меньший диаметр, большую стоимость и позволяют передачу информации на большие расстояния. Поскольку световые импульсы могут двигаться в одном направлении, системы на базе оптоволоконных кабелей должны иметь входящий кабель и исходящий кабель для каждого сегмента. Оптоволоконный кабель требует специальных коннекторов и высококвалифицированной установки.

4.3. Кабельные системы Ethernet

10Base-T, 100Base-TX

Неэкранированная витая пара (Unshielded Twisted Pair – UTP) – это кабель из скрученных пар проводов.

Характеристики кабеля:

– диаметр проводников 0.4 – 0.6 мм (22~26 AWG), 4 скрученных пары (8 проводников, из которых для 10Base-T и 100Base-TX используются только 4). Кабель должен иметь категорию 3 или 5 и качество data grade или выше;

– максимальная длина сегмента 100 м;

– разъемы восьми контактные RJ-45.

10Base2

– Тонкий коаксиальный кабель;

– Характеристики кабеля: диаметр 0.2 дюйма, RG-58A/U 50 Ом;

– Приемлемые разъемы – BNC;

– Максимальная длина сегмента – 185 м;

– Минимальное расстояние между узлами – 0.5 м;

– Максимальное число узлов в сегменте – 30.

10Base5

– Толстый коаксиальный кабель;

– Волновое сопротивление – 50 Ом;

– Максимальная длина сегмента – 500 метров;

– Минимальное расстояние между узлами –: 2.5 м;

– Максимальное число узлов в сегменте – 100.

4.4. Беспроводные технологии

Методы беспроводной технологии передачи данных (Radio Waves) являются удобным, а иногда незаменимым средством связи.

Беспроводные технологии различаются по типам сигнала, частоте (большая частота означает большую скорость передачи) и расстоянию передачи. Большое значение имеют помехи и стоимость. Можно выделить три основных типа беспроводной технологии:

- радиосвязь;
- связь в микроволновом диапазоне;
- инфракрасная связь.

Радиосвязь

Технологии радиосвязи пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Она используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость и чувствительна к электронному и атмосферному наложению, а также подвержена перехватам, поэтому требует шифрования для обеспечения уровня безопасности.

Связь в микроволновом диапазоне

Передача данных в микроволновом диапазоне (Microwaves) использует высокие частоты и применяется как на коротких, так и на больших расстояниях. Главное ограничение заключается в том, чтобы передатчик и приемник были в зоне прямой видимости. Используется в местах, где использование физического носителя затруднено. Передача данных в микроволновом диапазоне при использовании спутников может быть очень дорогой.

Инфракрасная связь

Инфракрасные технологии (Infrared transmission), функционируют на очень высоких частотах, приближающихся к частотам видимого света. Они могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. При инфракрасной связи обычно используют светодиоды (LED – *Light*

Emitting Diode) для передачи инфракрасных волн приемнику. Инфракрасная передача ограничена малым расстоянием в прямой зоне видимости и может быть использована в офисных зданиях.

4.5. Контрольные вопросы

1. Перечислить основные компоненты сети.
2. Как подразделяются компьютеры в сети?
3. Дать определение рабочей станции.
4. Чем отличается рабочая станция в сети от локального компьютера?
5. Что такое файловый сервер?
6. Какие бывают файловые серверы?
7. Какое назначение первичного контролера домена в сети?
8. Для чего используется вторичный контролера домена?
9. Что такое Proxy-сервер?
10. Какая информация хранится на сервере баз данных?
11. Достаточно ли одного сервера баз данных в сети с клиент-серверной архитектурой?
12. Может ли сервер баз данных и Web-сервер размещаться на одном компьютере?
13. Перечислить сетевое программное обеспечение рабочей станции.
14. Какое назначение СОС?
15. Перечислить наиболее известные сетевые операционные системы.
16. Чем различаются типы сетевых адаптеров?
17. Какую технологию поддерживают последние типы сетевых адаптеров?
18. Что такое сетевая операционная система?
19. Перечислить сетевое программное обеспечение и его назначение.
20. Для чего используется защита данных?
21. Что дает использование паролей и ограничение доступа?
22. Перечислить основные функции сетевых протоколов.
23. Для какой цели используется Web-сервер?

24. Какой сервер необходим для подключения к сети Internet?
25. Какое сетевое оборудование используется для связи между сегментами ЛВС?
26. Что такое физическая среда?
27. Что может быть использовано в качестве физической среды передачи данных?
28. Какие вопросы при организации сети решаются на физическом уровне?
29. Что такое кабель?
30. Что такое линии связи?
31. Дать определение каналов связи.
32. Какие проблемы существуют при организации каналов связи?
33. Перечислить типы кабелей, используемых для передачи данных в сети.
34. Каково назначение структурированной кабельной системы?
35. На какие классы подразделяются кабельные системы?
36. Что такое 10BaseT?
37. Какой кабель используется в технологии 10Base2?
38. Какой кабель используется в технологии 10Base5?
39. Назвать какие типы кабелей используют для передачи данных в сети?
40. Какие известны кабельные системы Ethernet?
41. Какие существуют типы оптоволоконных кабелей?
42. Какие известны технологи беспроводной передачи данных?
43. В каких случаях используется инфракрасная связь?
44. Назовите преимущества использования радиосвязи.

5. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К СЕТЯМ

При организации и эксплуатации сети важными требованиями при работе являются следующие [1]:

- производительность;
- надежность и безопасность;
- расширяемость и масштабируемость;
- прозрачность;
- поддержка разных видов трафика;
- управляемость;
- совместимость.

5.1. Производительность

Производительность – это характеристика сети, позволяющая оценить, насколько быстро информация передающей рабочей станции достигнет до приемной рабочей станции.

На производительность сети влияют следующие характеристики сети:

- конфигурация;
- скорость передачи данных;
- метод доступа к каналу;
- топология сети;
- технология.

Если производительность сети перестает отвечать предъявляемым к ней требованиям, то администратор сети может прибегнуть к различным приемам:

- изменить конфигурацию сети таким образом, чтобы структура сети более соответствовала структуре информационных потоков;
- перейти к другой модели построения распределенных приложений, которая позволила бы уменьшить сетевой трафик;
- заменить мосты более скоростными коммутаторами.

Но самым радикальным решением в такой ситуации является переход на более скоростную технологию. Если в сети используются традиционные технологии Ethernet или Token Ring, то переход на Fast Ethernet, FDDI или 100VG-AnyLAN позволит сразу в 10 раз увеличить пропускную способность каналов.

С ростом масштаба сетей возникла необходимость в повышении их производительности. Одним из способов достижения этого стала их микросегментация. Она позволяет уменьшить число пользователей на один сегмент и снизить объем широковещательного трафика, а значит, повысить производительность сети.

Первоначально для микросегментации использовались маршрутизаторы, которые, вообще говоря, не очень приспособлены для этой цели. Решения на их основе были достаточно дорогостоящими и отличались большой временной задержкой и невысокой пропускной способностью. Более подходящими устройствами для микросегментации сетей стали коммутаторы. Благодаря относительно низкой стоимости, высокой производительности и простоте в использовании они быстро завоевали популярность.

Таким образом, сети стали строить на базе коммутаторов и маршрутизаторов. Первые обеспечивают высокоскоростную пересылку трафика между сегментами, входящими в одну подсеть, а вторые передают данные между подсетями, ограничивали распространение широковещательного трафика, решали задачи безопасности и т. д.

Виртуальные ЛВС (VLAN) обеспечивают возможность создания логических групп пользователей в масштабе корпоративной сети. Виртуальные сети позволяют организовать работу в сети более эффективно.

5.2. Надежность и безопасность

Важнейшей характеристикой вычислительных сетей является надежность. Повышение надежности основано на принципе

предотвращения неисправностей путем снижения интенсивности отказов и сбоев за счет применения электронных схем и компонентов с высокой и сверхвысокой степенью интеграции, снижения уровня помех, облегченных режимов работы схем, обеспечение тепловых режимов их работы, а также за счет совершенствования методов сборки аппаратуры.

Отказоустойчивость – это такое свойство вычислительной системы, которое обеспечивает ей как логической машине возможность продолжения действий, заданных программой, после возникновения неисправностей. Введение отказоустойчивости требует избыточного аппаратного и программного обеспечения. Направления, связанные с предотвращением неисправностей и отказоустойчивостью, основные в проблеме надежности. На параллельных вычислительных системах достигается как наиболее высокая производительность, так и, во многих случаях, очень высокая надежность. Имеющиеся ресурсы избыточности в параллельных системах могут гибко использоваться как для повышения производительности, так и для повышения надежности.

Следует помнить, что понятие надежности включает не только аппаратные средства, но и программное обеспечение. Главной целью повышения надежности систем является целостность хранимых в них данных.

Безопасность – одна из основных задач, решаемых любой нормальной компьютерной сетью. Проблему безопасности можно рассматривать с разных сторон – злонамеренная порча данных, конфиденциальность информации, несанкционированный доступ, хищения и т.п.

Обеспечить защиту информации в условиях локальной сети всегда легче, чем при наличии на фирме десятка автономно работающих компьютеров. Практически в вашем распоряжении один инструмент – резервное копирование (backup). Для простоты давайте называть этот процесс резервированием. Суть его состоит в создании в безопасном месте полной копии данных, обновляемой регулярно и как можно чаще. Для персонального компьютера более или менее безопасным носителем

служат дискеты. Возможно использование стримера, но это уже дополнительные затраты на аппаратуру.

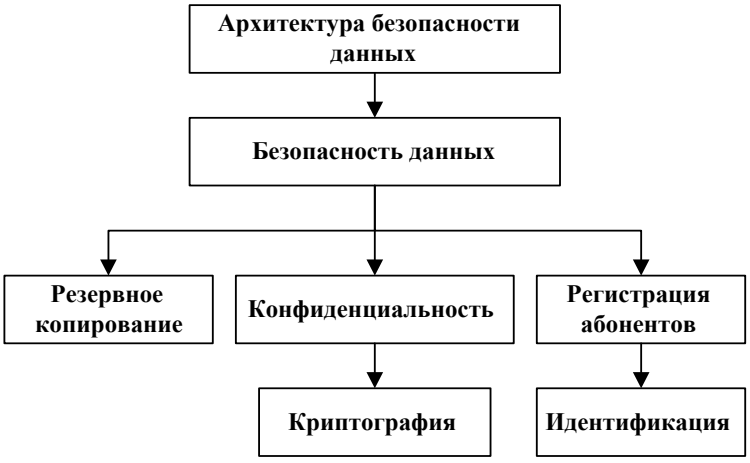

Рис. 5.1. Задачи обеспечения безопасности данных

Легче всего обеспечить защиту данных от самых разных неприятностей в случае сети с выделенным файловым сервером. На сервере сосредоточены все наиболее важные файлы, а уберечь одну машину куда проще, чем десять. Концентрированность данных облегчает и резервирование, так как не требуется их собирать по всей сети.

Экранированные линии позволяют повысить безопасность и надежность сети. Экранированные системы гораздо более устойчивы к внешним радиочастотным полям.

5.3. Прозрачность

Прозрачность – это такое состояние сети, когда пользователь, работая в сети, не видит ее.

Коммуникационная сеть является прозрачной относительно проходящей сквозь нее информации, если выходной поток битов, в точности повторяет входной поток. Но сеть может быть непрозрачной во времени, если из-за меняющихся размеров очередей блоков данных изменяется и время прохождения различных блоков через узлы

коммутации. Прозрачность сети по скорости передачи данных указывает, что данные можно передавать с любой нужной скоростью.

Если в сети по одним и тем же маршрутам передаются информационные и управляющие (синхронизирующие) сигналы, то говорят, что сеть прозрачна по отношению к типам сигналов.

Если передаваемая информация может кодироваться любым способом, то это означает, что сеть прозрачна для любых методов кодировок.

Прозрачная сеть является простым решением, в котором для взаимодействия локальных сетей, расположенных на значительном расстоянии друг от друга, используется принцип *Plug-and-play*.

Прозрачное соединение. Служба *прозрачных* локальных сетей обеспечивает сквозное (end-to-end) соединение, связывающее между собой удаленные локальные сети. Привлекательность данного решения состоит в том, что эта служба объединяет удаленные друг от друга на значительное расстояние узлы как части локальной сети. Поэтому не нужно вкладывать средства в изучение новых технологий и создание территориально распределенных сетей (Wide-Area Network – WAN). Пользователям требуется только поддерживать локальное соединение, а провайдер службы прозрачных сетей обеспечит беспрепятственное взаимодействие узлов через сеть масштаба города (Metropolitan-Area Network – MAN) или сеть WAN. Службы *Прозрачной* локальной сети имеют много преимуществ. Например, пользователь может быстро и безопасно передавать большие объемы данных на значительные расстояния, не обременяя себя сложностями, связанными с работой в сетях WAN.

5.4. Поддержка разных видов трафика

Трафик в сети складывается случайным образом, однако в нем отражены и некоторые закономерности. Как правило, некоторые пользователи, работающие над общей задачей, (например, сотрудники

одного отдела), чаще всего обращаются с запросами либо друг к другу, либо к общему серверу, и только иногда они испытывают необходимость доступа к ресурсам компьютеров другого отдела. Желательно, чтобы структура сети соответствовала структуре информационных потоков. В зависимости от сетевого трафика компьютеры в сети могут быть разделены на группы (сегменты сети). Компьютеры объединяются в группу, если большая часть порождаемых ими сообщений, адресована компьютерам этой же группы.

Для разделения сети на сегменты используются мосты и коммутаторы. Они экранируют локальный трафик внутри сегмента, не передавая за его пределы никаких кадров, кроме тех, которые адресованы компьютерам, находящимся в других сегментах. Таким образом, сеть распадается на отдельные подсети. Это позволяет более рационально выбирать пропускную способность имеющихся линий связи, учитывая интенсивность трафика внутри каждой группы, а также активность обмена данными между группами.

Однако локализация трафика средствами мостов и коммутаторов имеет существенные ограничения. С другой стороны, использование механизма виртуальных сегментов, реализованного в коммутаторах локальных сетей, приводит к полной локализации трафика; такие сегменты полностью изолированы друг от друга, даже в отношении широковещательных кадров. Поэтому в сетях, построенных только на мостах и коммутаторах, компьютеры, принадлежащие разным виртуальным сегментам, не образуют единой сети.

Для того чтобы эффективно консолидировать различные виды трафика в сети ATM, требуется специальная предварительная подготовка (адаптация) данных, имеющих различный характер: кадры – для цифровых данных, сигналы импульсно-кодовой модуляции – для голоса, потоки битов – для видео. Эффективная консолидация трафика требует также учета и использования статистических вариаций интенсивности различных типов трафика.

5.5. Управляемость

ISO внесла большой вклад в стандартизацию сетей. Модель управления сети является основным средством для понимания главных функций систем управления сети. Эта модель состоит из 5 концептуальных областей:

- управление эффективностью;
- управление конфигурацией;
- управление учетом использования ресурсов;
- управление неисправностями;
- управление защитой данных.

Управление эффективностью

Цель управления эффективностью – измерение и обеспечение различных аспектов эффективности сети для того, чтобы межсетевая эффективность могла поддерживаться на приемлемом уровне. Примерами переменных эффективности, которые могли бы быть обеспечены, являются пропускная способность сети, время реакции пользователей и коэффициент использования линии.

Управление эффективностью включает несколько этапов:

1. Сбор информации об эффективности по тем переменным, которые представляют интерес для администраторов сети;

2. Анализ информации для определения нормальных (базовая строка) уровней;

3. Определение соответствующих порогов эффективности для каждой важной переменной таким образом, что превышение этих порогов указывает на наличие проблемы в сети, достойной внимания.

Управление конфигурацией

Цель управления конфигурацией – контролирование информации о сетевой и системной конфигурации для того, чтобы можно было отслеживать и управлять воздействием на работу сети различных

версий аппаратных и программных элементов. Т.к. все аппаратные и программные элементы имеют эксплуатационные отклонения, погрешности (или то и другое вместе), которые могут влиять на работу сети, такая информация важна для поддержания гладкой работы сети.

Каждое устройство сети располагает разнообразной информацией о версиях, ассоциируемых с ним. Чтобы обеспечить легкий доступ, подсистемы управления конфигурацией хранят эту информацию в базе данных. Когда возникает какая-нибудь проблема, в этой базе данных может быть проведен поиск ключей, которые могли бы помочь решить эту проблему.

Управление учетом использования ресурсов

Цель управления учетом использования ресурсов – измерение параметров использования сети, чтобы можно было соответствующим образом регулировать ее использование индивидуальными или групповыми пользователями. Такое регулирование минимизирует число проблем в сети (т.к. ресурсы сети могут быть поделены исходя из возможностей источника) и максимизирует равнодоступность к сети для всех пользователей.

Управление неисправностями

Цель управления неисправностями – выявить, зафиксировать, уведомить пользователей и (в пределах возможного) автоматически устранить проблемы в сети, с тем чтобы эффективно поддерживать работу сети. Так как неисправности могут привести к простоям или недопустимой деградации сети, управление неисправностями, по всей вероятности, является наиболее широко используемым элементом модели управления сети ISO.

Управление неисправностями включает в себя несколько шагов:

1. Определение симптомов проблемы;
2. Изолирование проблемы;
3. Устранение проблемы;

4. Проверка устранения неисправности на всех важных подсистемах;

5. Регистрация обнаружения проблемы и ее решения.

Управление защитой данных

Цель управления защитой данных – контроль доступа к сетевым ресурсам в соответствии с местными руководящими принципами, чтобы сделать невозможными саботаж сети и доступ к чувствительной информации лицам, не имеющим соответствующего разрешения. Например, одна из подсистем управления защитой данных может контролировать регистрацию пользователей ресурса сети, отказывая в доступе тем, кто вводит коды доступа, не соответствующие установленным.

Подсистемы управления защитой данных работают путем разделения источников на санкционированные и несанкционированные области. Для некоторых пользователей доступ к любому источнику сети является несоответствующим.

Подсистемы управления защитой данных выполняют следующие функции:

– идентифицируют чувствительные ресурсы сети (включая системы, файлы и другие объекты);

– определяют отображения в виде карт между чувствительными источниками сети и набором пользователей;

– контролируют точки доступа к чувствительным ресурсам сети;

– регистрируют несоответствующий доступ к чувствительным ресурсам сети.

5.6. Совместимость

Концепция программной совместимости впервые в широких масштабах была применена разработчиками системы IBM/360. Основная задача при проектировании всего ряда моделей этой системы

заключалась в создании такой архитектуры, которая была бы одинаковой с точки зрения пользователя для всех моделей системы независимо от цены и производительности каждой из них. Огромные преимущества такого подхода, позволяющего сохранять существующий задел программного обеспечения при переходе на новые (как правило, более производительные) модели, были быстро оценены как производителями компьютеров, так и пользователями, и начиная с этого времени практически все фирмы-поставщики компьютерного оборудования взяли на вооружение эти принципы, поставляя серии совместимых компьютеров. Следует заметить, что со временем даже самая передовая архитектура неизбежно устаревает и возникает потребность внесения радикальных изменений в архитектуру и способы организации вычислительных систем.

В настоящее время одним из наиболее важных факторов, определяющих современные тенденции в развитии информационных технологий, является ориентация компаний-поставщиков компьютерного оборудования на рынок прикладных программных средств.

Этот переход выдвинул ряд новых требований. Прежде всего, такая вычислительная среда должна позволять гибко менять количество и состав аппаратных средств и программного обеспечения в соответствии с меняющимися требованиями решаемых задач. Во-вторых, она должна обеспечивать возможность запуска одних и тех же программных систем на различных аппаратных платформах, т.е. обеспечивать мобильность программного обеспечения. В-третьих, эта среда должна гарантировать возможность применения одних и тех же человеко-машинных интерфейсов на всех компьютерах, входящих в неоднородную сеть. В условиях жесткой конкуренции производителей аппаратных платформ и программного обеспечения сформировалась концепция открытых систем, представляющая собой совокупность стандартов на различные компоненты вычислительной среды,

предназначенных для обеспечения мобильности программных средств в рамках неоднородной, распределенной вычислительной системы.

5.7. Контрольные вопросы

1. Какие основные требования предъявляются к сетям?
2. Что такое производительность сети?
3. Какие характеристики влияют на производительность сети?
4. Какие есть способы повышения производительности сетей?
5. Как обеспечить высокоскоростную пересылку трафика?
6. Чем обеспечивается надежность сети?
7. Что такое отказоустойчивость?
8. Перечислить задачи безопасности данных в сети.
9. Для какой цели используется резервное копирование?
10. Чем обеспечивается безопасность сетей в клиент-серверной архитектуре?
11. Для какой цели устанавливаются экранированные линии в сети?
12. Что такое прозрачность сетей?
13. В каком случае линия прозрачна по отношению к типам сигналов?
14. Что такое прозрачное соединение?
15. Что используется для разделения сети на сегменты?
16. Каким образом можно уменьшить трафик в сети?
17. Дать определение управляемости сетей и перечислить основные функции управления сетями.
18. Что включается в управление эффективностью?
19. Для какой цели используется управление неисправностями?
20. Для чего необходимо управление конфигурацией?
21. Какова цель управления защитой данных?
22. Какие функции подсистемы управления защитой данных?
23. Дайте определение понятия совместимости сетей.

6. СЕТЕВОЕ ОБОРУДОВАНИЕ

6.1. Сетевые адаптеры

Назначение

Сетевые адаптеры или NIC (Network Interface Card) – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях [7].

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

Компьютер, будь то сервер или рабочая станция, подключается к сети с помощью внутренней платы – сетевого адаптера (хотя бывают и внешние сетевые адаптеры, подключаемые к компьютеру через параллельный порт). Сетевой адаптер вставляется в гнездо материнской платы. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов. Сетевые адаптеры преобразуют параллельные коды, используемые внутри компьютера и представленные маломощными сигналами, в последовательный поток мощных сигналов для передачи данных по внешней сети. Сетевые адаптеры должны быть совместимы с кабельной системой сети, внутренней информационной шиной ПК и сетевой операционной системой.

Настройка сетевого адаптера и трансивера

Для работы ПК в сети надо правильно установить и настроить сетевой адаптер. Для адаптеров, отвечающих стандарту PnP, настройка производится автоматически. В ином случае необходимо настроить линию запроса на прерывание IRQ (Interrupt Request Line) и адрес ввода/вывода (Input/Output address).

Обычно сетевая карта работает с конфликтами, если двум устройствам назначен один и тот же ресурс (запроса на прерывание или адрес ввода/вывода). Сетевые карты поддерживают различные типы сетевых соединений. Физический интерфейс между самой сетевой картой и сетью называют трансивером (transceiver) – это устройство, которое как получает, так и посылает данные. Трансиверы на сетевых картах могут получать и посылать цифровые и аналоговые сигналы. Тип интерфейса, который использует сетевая карта, часто может быть физически определен на сетевой карте. Перемычки, или джамперы (маленькие перемычки, соединяющие два контакта), могут быть настроены для указания типа трансивера, который должна использовать сетевая карта в соответствии со схемой сети. Например, перемычка в одном положении может включить разъем RJ-45 для поддержки сети типа витая пара, в другом – поддержку внешнего трансивера.

Функции сетевых адаптеров

Сетевые адаптеры производят семь основных операций при приеме или передачи сообщения:

1. *Гальваническая развязка* с коаксиальным кабелем или витой парой. Для этой цели используются импульсные трансформаторы. Иногда дя развязки используются оптроны.

2. *Прием (передача) данных*. Данные передаются из ОЗУ ПК в адаптер или из адаптера в память ПК через программируемый канал ввода/вывода, канал прямого доступа или разделяемую память.

3. *Буферизация*. Для согласования скоростей пересылки данных в адаптер или из него со скоростью обмена по сети используются буфера.

Во время обработки в сетевом адаптере, данные хранятся в буфере. Буфер позволяет адаптеру осуществлять доступ ко всему пакету информации. Использование буферов необходимо для согласования между собой скоростей обработки информации различными компонентами ЛВС.

4. *Формирование пакета.* Сетевой адаптер должен разделить данные на блоки в режиме передачи (или соединить их в режиме приема) данных и оформить в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.

5. *Доступ к каналу связи.* Набор правил, обеспечивающих доступ к среде передачи. Выявление конфликтных ситуаций и контроль состояния сети.

6. *Идентификация своего адреса* в принимаемом пакете. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ.

7. *Преобразование* параллельного кода в последовательный код при передаче данных, и из последовательного кода в параллельный при приеме. В режиме передачи данные передаются по каналу связи в последовательном коде.

8. *Кодирование и декодирование данных.* На этом этапе должны быть сформированы электрические сигналы, используемые для представления данных. Большинство сетевых адаптеров для этой цели используют манчестерское кодирование. Этот метод не требует передачи синхронизирующих сигналов для распознавания единиц и нулей по уровням сигналов, а вместо этого для представления 1 и 0 используется перемена полярности сигнала.

9. *Передача или прием импульсов.* В режиме передачи закодированные электрические импульсы данных передаются в кабель (при приеме импульсы направляются на декодирование).

Сетевые адаптеры вместе с сетевым программным обеспечением способны распознавать и обрабатывать ошибки, которые могут возникнуть из-за электрических помех, коллизий или плохой работы оборудования.

Базовый, или физический, адрес

Некоторые сетевые адаптеры имеют возможность использовать оперативную память ПК в качестве буфера для хранения входящих и исходящих пакетов данных. Базовый адрес (Base Memory Address) представляет собой шестнадцатеричное число, которое указывает на адрес в оперативной памяти, где находится этот буфер. Важно выбрать базовый адрес без конфликтов с другими устройствами.

Типы сетевых адаптеров

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных – ISA, EISA, PCI, MCA.

Сетевые адаптеры различаются также по типу принятой в сети сетевой технологии – Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Различные типы сетевых адаптеров отличаются не только методами доступа к среде и протоколами, но еще и следующими параметрами:

- скорость передачи;
- объем буфера для пакета;
- тип шины;
- быстродействие шины;
- совместимость с различными микропроцессорами;
- использование прямого доступа к памяти (DMA);
- адресация портов ввода/вывода и запросов прерывания;
- конструкция разъема.

Наиболее известны следующие типы адаптеров:

Адаптеры Ethernet представляют собой плату, которая вставляется в свободный слот материнской (системной) платы компьютера. Чаще всего адаптеры Ethernet имеют для связи с сетью два внешних разъема: для коаксиального кабеля (разъем BNC) и для кабеля на витой паре. Для выбора типа кабеля применяются перемычки или переключатели, которые устанавливаются перед подключением адаптера к сети.

Адаптеры Fast Ethernet производятся изготовителями с учетом определенного типа среды передачи. Сетевой кабель при этом подключается непосредственно к адаптеру (без трансивера).

Оптические адаптеры стандарта 10BASE-FL могут устанавливаться в компьютеры с шинами ISA, PCI, MCA. Эти адаптеры позволяют отказаться от внешних преобразователей среды и от микротрансиверов. При установке этих адаптеров возможна реализация полнодуплексного режима обмена информацией. Для повышения универсальности в оптических адаптерах сохраняется возможность соединения по витой паре с разъемом RJ-45.

Для спецификации 100BASE-FX соединение концентратора и адаптера по оптоволокну осуществляется с использованием оптических соединителей типа SC или ST. Выбор типа оптического соединителя (SC или ST) зависит от того, новая или старая это инсталляция. Для этой

спецификации выпускаются сетевые адаптеры, совместимые с шиной PCI. Адаптеры способны поддерживать как полудуплексный, так и полнодуплексный режим работы. Для облегчения настройки и эксплуатации на переднюю панель адаптера вынесено несколько индикаторов состояния. Кроме того, существуют модели адаптеров, способные работать как по одномодовому, так и по многомодовому оптоволоконному кабелю.

Сетевые адаптеры для технологии Gigabit Ethernet предназначены для установки в сервера и мощные рабочие станции. Для повышения эффективности работы они способны поддерживать полнодуплексный режим обмена информацией.

Адаптеры FDDI могут использоваться на разнообразных рабочих станциях и в устройствах межсетевого взаимодействия – мостах и маршрутизаторах. Существуют адаптеры FDDI, предназначенные для работы со всеми распространенными шинами: ISA, EISA, VESA Local Bus (VLB) и т. д. В сети FDDI такие устройства, как рабочие станции или мосты и подсоединяются к кольцу через адаптеры одного из двух типов: с двойным (DAS) или одиночным (SAS) подключением. Адаптеры DAS осуществляют физическое соединение устройств как с первичным, так и с вторичным кольцом, что повышает отказоустойчивость сети. Такой адаптер имеет два разъема (розетки) оптического интерфейса. Адаптеры SAS подключают рабочие станции к концентратору FDDI через одиночную оптоволоконную линию в звездообразной топологии. Эти адаптеры представляют собой плату, на которой наряду с электронными компонентами установлен оптический трансивер с разъемом (розеткой) оптического интерфейса.

6.2. Повторители и концентраторы

Основная функция *повторителя* (repeater), как это следует из его названия, – повторение сигналов, поступающих на его порт [7]. Повторитель улучшает электрические характеристики сигналов и их

синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети узлами.

Многопортовый повторитель часто называют *концентратором* (concentrator) или *хабом* (hub), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть. Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть.

Концентратор или Hub представляет собой сетевое устройство, действующее на физическом уровне сетевой модели OSI.

Отрезки кабеля, соединяющие два компьютера или какие либо два других сетевых устройства, называются *физическими сегментам,* поэтому концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентратор – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала. Так как потоки входных данных в концентраторе больше выходного потока, то главной его задачей является концентрация данных. При этом возможны ситуации, когда число блоков данных, поступающее на входы концентратора, превышает его возможности. Тогда концентратор ликвидирует часть этих блоков.

Ядром концентратора является процессор. Для объединения входной информации чаще всего используется множественный доступ с разделением времени. Функции, выполняемые концентратором, близки к задачам, возложенным на мультиплексор. Наращиваемые (модульные) концентраторы позволяют выбирать их компоненты, не думая о совместимости с уже используемыми. Современные концентраторы имеют порты для подключения к разнообразным локальным сетям.

Концентратор является активным оборудованием. Концентратор служит центром (шиной) звездообразной конфигурации сети и

обеспечивает подключение сетевых устройств. В концентраторе для каждого узла (ПК, принтеры, серверы доступа, телефоны и пр.) должен быть предусмотрен отдельный порт.

Наращиваемые концентраторы представляют собой отдельные модули, которые объединяются при помощи быстродействующей системы связи. Такие концентраторы предоставляют удобный способ поэтапного расширения возможностей и мощности ЛВС.

Концентратор осуществляет электрическую развязку отрезков кабеля до каждого узла, поэтому короткое замыкание на одном из отрезков не выведет из строя всю ЛВС.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – *логический сегмент*. Логический сегмент также называют доменом коллизий, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что, какую бы сложную структуру ни образовывали концентраторы, например путем иерархического соединения (рис. 6.1), все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

На рис. 6.2 показан внешний вид концентратора. Концентраторы поддерживают технологию plug and play и не требуют какой-либо установки параметров. Необходимо просто спланировать свою сеть и вставить разъемы в порты хаба и компьютеров.

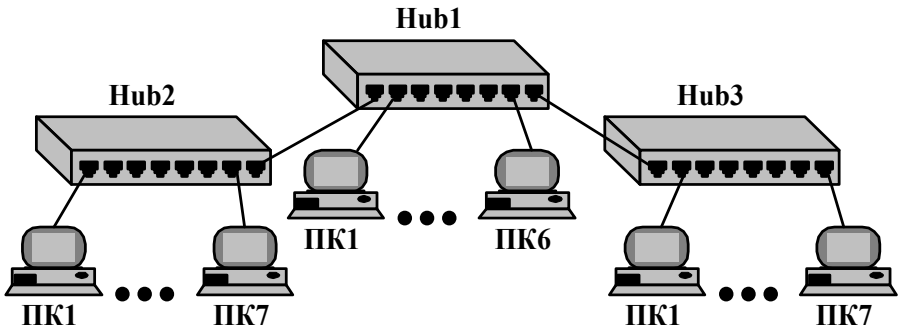

Рис. 6.1. Логический сегмент, построенный с использованием концентраторов

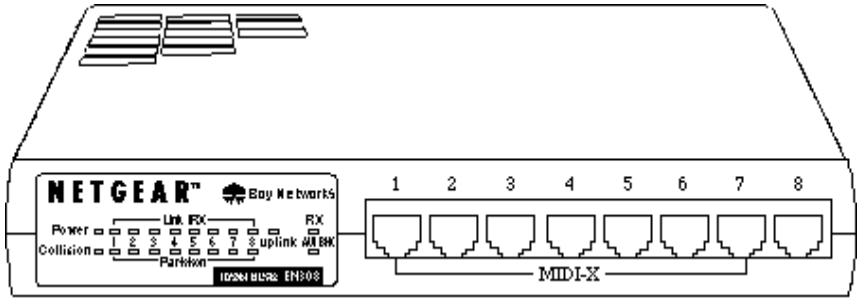

Рис. 6.2. Внешний вид концентратора

При выборе места для установки концентратора принимаются во внимание следующие аспекты:

- местоположение;
- расстояния;
- питание.

Выбор места установки концентратора является наиболее важным этапом планирования небольшой сети. Хаб разумно расположить вблизи геометрического центра сети (на одинаковом расстоянии от всех компьютеров). Такое расположение позволит минимизировать расход кабеля. Длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100 м.

Концентратор можно поставить на стол или закрепить его на стене с помощью входящих в комплект хаба скоб. Установка хаба на стене позволяет упростить подключение кабелей, если они уже проложены в офисе.

При планировании сети есть возможность наращивания (каскадирования) хабов.

Преимущества концентратора

Концентраторы имеют много преимуществ. Во-первых, в сети используется топология звезда, при которой соединения с компьютерами образуют лучи, а хаб является центром звезды. Такая топология упрощает установку и управление сети. Любые перемещения компьютеров или добавление в сеть новых узлов при такой топологии весьма несложно выполнить. Кроме того, эта топология значительно надежнее, поскольку при любом повреждении кабельной системы сеть сохраняет работоспособность (перестает работать лишь поврежденный луч). Светодиодные индикаторы хаба позволяют контролировать состояние сети и легко обнаруживать неполадки.

Различные производители концентраторов реализуют в своих устройствах различные наборы вспомогательных функций, но наиболее часто встречаются следующие:

– объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно) в единый логический сегмент;

– автосегментация портов – автоматическое отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т. п.);

– поддержка между концентраторами резервных связей, которые используются при отказе основных;

– защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютера с адресом назначения);

– поддержка средств управления сетями – протокола SNMP, баз управляющей информации MIB.

6.3. Мосты и коммутаторы

Мост (bridge) – ретрансляционная система, соединяющая каналы передачи данных [7].

В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. Мост преобразует физический (1A, 1B) и канальный (2A, 2B) уровни различных типов (рис. 6.3). Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий.

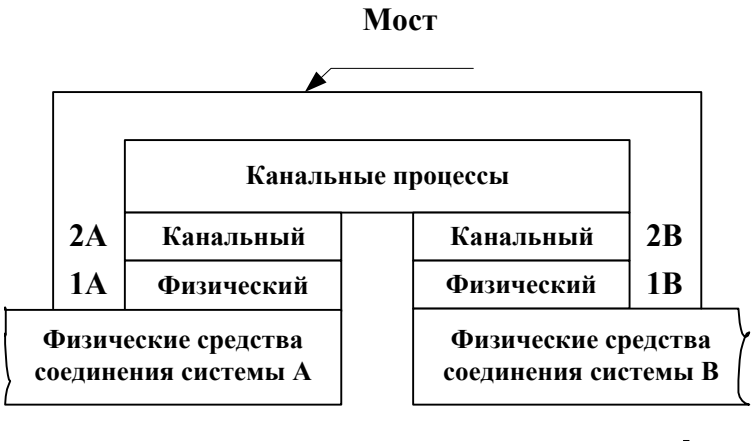

Рис. 6.3. Структура моста

Мост (bridge), а также его быстродействующий аналог – *коммутатор* (switching hub), делят общую среду передачи данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор,

а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

Мосты могут соединять сегменты, использующие разные типы носителей, например 10BaseT (витая пара) и 10Base2 (тонкий коаксиальный кабель). Они могут соединять сети с разными методами доступа к каналу, например сети Ethernet (метод доступа CSMA/CD) и Token Ring (метод доступа TPMA).

Различие между мостом и коммутатором

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно.

Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.

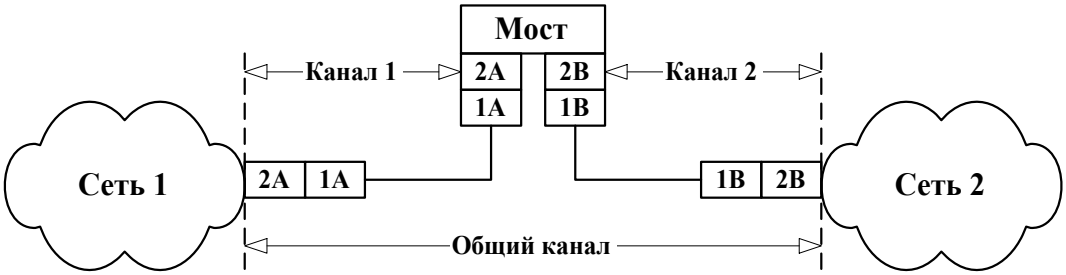

Рис. 6.4. Соединение двух сетей при помощи двух каналов

Когда появились первые устройства, позволяющие разъединять сеть на несколько доменов коллизий (по сути фрагменты ЛВС, построенные на hub-ax), они были двух портовыми и получили название мостов (bridge-ей). По мере развития данного типа оборудования, они стали многопортовыми и получили название коммутаторов (switch-ей). Некоторое время оба понятия существовали одновременно, а позднее

вместо термина «мост» стали применять «коммутатор». Далее в этой теме будет использоваться термин «коммутатор» для обозначения этих обеих разновидностей устройств, поскольку все сказанное ниже в равной степени относится и к мостам, и к коммутаторам. Следует отметить, что в последнее время локальные мосты полностью вытеснены коммутаторами.

Нередки случаи, когда необходимо соединить локальные сети, в которых различаются лишь протоколы физического и канального уровней. Протоколы остальных уровней в этих сетях приняты одинаковыми. Такие сети могут быть соединены мостом. Часто мосты наделяются дополнительными функциями. Такие мосты обладают определенным *интеллектом* (интеллектом в сетях называют действия, выполняемые устройствами) и фильтруют сквозь себя блоки данных, адресованные абонентским системам, расположенным в той же сети. Для этого в памяти каждого моста имеются адреса систем, включенных в каждую из сетей. Блоки, проходящие через *интеллектуальный* мост, дважды проверяются, на входе и выходе. Это позволяет предотвращать появление ошибок внутри моста.

Мосты не имеют механизмов управления потоками блоков данных. Поэтому может оказаться, что входной поток блоков окажется большим, чем выходной. В этом случае мост не справится с обработкой входного потока, и его буферы могут переполняться. Чтобы этого не произошло, избыточные блоки выбрасываются. Специфические функции выполняет мост в радиосети. Здесь он обеспечивает взаимодействие двух радиоканалов, работающих на разных частотах. Его именуют *ретранслятором*.

Мосты (bridges) оперируют данными на высоком уровне и имеют совершенно определенное назначение. Во-первых, они предназначены для соединения сетевых сегментов, имеющих различные физические среды, например для соединения сегмента с оптоволоконным кабелем и сегмента с коаксиальным кабелем. Мосты также могут быть

использованы для связи сегментов, имеющих различные протоколы низкого уровня (физического и канального).

Коммутатор

Коммутатор (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных.

В коммуникационной сети коммутатор является ретрансляционной системой (система, предназначенная для передачи данных или преобразования протоколов), обладающей свойством прозрачности (т.е. коммутация осуществляется здесь без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение.

Вначале коммутаторы использовались лишь в территориальных сетях. Затем они появились и в локальных сетях, например, частные учрежденческие коммутаторы. Позже появились коммутируемые локальные сети. Их ядром стали коммутаторы локальных сетей.

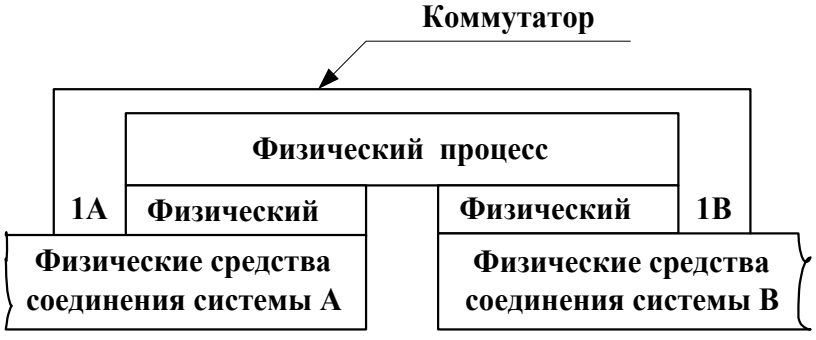

Рис. 6.5. Структура коммутатора

Коммутатор (Switch) может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп. Он направляет пакеты данных между узлами ЛВС. Каждый

коммутируемый сегмент получает доступ к каналу передачи данных без конкуренции и видит только тот трафик, который направляется в его сегмент. Коммутатор должен предоставлять каждому порту возможность соединения с максимальной скоростью без конкуренции со стороны других портов (в отличие от совместно используемого концентратора). Обычно в коммутаторах имеются один или два высокоскоростных порта, а также хорошие инструментальные средства управления. Коммутатором можно заменить маршрутизатор, дополнить им наращиваемый маршрутизатор или использовать коммутатор в качестве основы для соединения нескольких концентраторов. Коммутатор может служить отличным устройством для направления трафика между концентраторами ЛВС рабочей группы и загруженными файл-серверами.

Коммутатор локальной сети

Коммутатор локальной сети (local-area network switch) – устройство, обеспечивающее взаимодействие сегментов одной либо группы локальных сетей.

Коммутатор локальной сети, как и обычный коммутатор, обеспечивает взаимодействие подключенных к нему локальных сетей (рис. 6.6). Но в дополнение к этому он осуществляет преобразование интерфейсов, если соединяются различные типы сегментов локальной сети. Чаще всего это сети Ethernet, кольцевые сети IBM, сети с оптоволоконным распределенным интерфейсом данных.

Рис. 6.6. Схема подключения локальных сетей к коммутаторам

В перечень функций, выполняемых коммутатором локальной сети, входят:

- обеспечение сквозной коммутации;
- наличие средств маршрутизации;
- поддержка простого протокола управления сетью;
- имитация моста либо маршрутизатора;
- организация виртуальных сетей;
- скоростная ретрансляция блоков данных.

6.4. Маршрутизаторы

Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части.

Каждый маршрутизатор реализует протоколы *физического* (1A, 1B), *канального* (2A, 2B) и *сетевого* (3A, 3B) уровней, как показано на рис. 6.7. Специальные сетевые процессы соединяют части коммутатора в единое целое. Физический, канальный и сетевой протоколы в разных сетях различны. Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые осуществляют необходимое преобразование указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей.

Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных.

Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии. Благодаря этому, выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю. Маршрутизаторы обеспечивают также соединение административно независимых коммуникационных сетей.

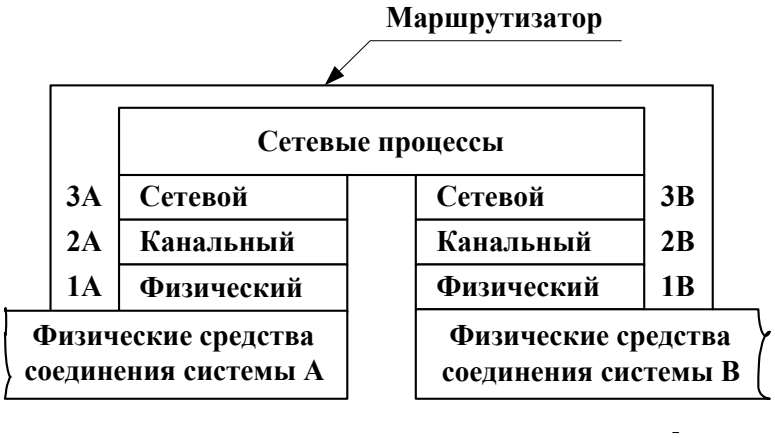

Рис. 6.7. Структура маршрутизатора

Архитектура маршрутизатора также используется при создании узла коммутации пакетов.

Различие между маршрутизаторами и мостами

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных на сети. Так как маршрутизаторы работают на сетевом уровне, они могут соединять сети, использующие разную сетевую архитектуру, методы доступа к каналам связи и протоколы.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами.

Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета.

В поле зрения маршрутизаторов находятся только пакеты, адресованные к ним предыдущими маршрутизаторами, в то время как мосты должны обрабатывать все пакеты сообщений в сегменте сети, к которому они подключены.

Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на уровень выше,

чем мосты (сетевой уровень модели OSI). Маршрутизаторы часто используются для связи между сегментами с одинаковыми протоколами высокого уровня. Наиболее распространенным транспортным протоколом, который используют маршрутизаторы, является IPX фирмы Novell или TCP фирмы Microsoft.

Необходимо запомнить, что для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан. При связывании сетей с различными протоколами лучше использовать мосты. Для управления загруженностью трафика сегмента сети также можно использовать мосты.

6.5. Шлюзы

Шлюз (gateway) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей.

Рис. 6.8. Структура шлюза

Шлюз является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения.

В тех случаях, когда соединяются информационные сети, то в них часть уровней может иметь одни и те же протоколы. Тогда сети соединяются не при помощи шлюза, а на основе более простых ретрансляционных систем, именуемых маршрутизаторами и мостами.

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать для соединения сети с протоколом TCP/IP и большой ЭВМ со стандартом SNA. Эти две архитектуры не имеют ничего общего, и потому требуется полностью переводить весь поток данных, проходящих между двумя системами.

В качестве шлюза обычно используется выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать нескольким системам в сети. Другой функцией шлюзов является преобразование протоколов. При получении сообщения IPX/SPX для клиента TCP/IP шлюз преобразует сообщения в протокол TCP/IP.

6.6. Контрольные вопросы

1. Назначение сетевого адаптера.
2. Какие параметры необходимо устанавливать у сетевого адаптера?
3. Перечислить функции сетевых адаптеров.
4. Что такое физический адрес адаптера?
5. Как определить физический адрес адаптера?
6. Какие есть типы сетевых адаптеров?
7. На каком уровне сетевой модели OSI используется сетевой адаптер?
8. Каково назначение повторителя?
9. В каких случаях ставят сетевой повторитель?

10. Что такое сетевой концентратор и каково его назначение?
11. На каком уровне сетевой модели OSI используется сетевой концентр?
12. Назначение моста.
13. На каком уровне сетевой модели OSI используется мост?
14. Какие сегменты сети может соединять мост?
15. Назначение коммутатора. На каком уровне сетевой модели OSI используется коммутатор?
16. Каково различие между мостом и коммутатором?
17. Назначение маршрутизатора.
18. На каком уровне сетевой модели OSI используется маршрутизатор?
19. Каково различие между маршрутизаторами и мостами?
20. Что такое шлюз и каково его назначение?
21. На каком уровне сетевой модели OSI используется шлюз?

ЗАКЛЮЧЕНИЕ

Таким образом, в настоящем учебном пособии даны базовые знания по организации и функционированию сетей. Рассмотрены общие понятия компьютерных сетей, их структура, сетевые компоненты; приведены виды топологии, используемые для физического соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных и передача данных в сети, рассмотренная на основе эталонной базовой модели, разработанной Международной организацией по стандартам взаимодействия открытых сетей; описаны правила и процедуры передачи данных между информационными системами; приведены типы сетевого оборудования, их назначение и принципы работы; рассмотрены принципы межсетевого взаимодействия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Жеретинцева Н.Н. Курс лекций по компьютерным сетям. – Владивосток: ДВГМА, 2000. – 158 с.
2. Карпов, Д.И. Статическая IP-маршрутизация [Электронный ресурс]. – http://www.citforum.ru/internet/tifamily/iproutng.shtml. (Дата обращения 15.03.1012)
3. Комер, Д. Межсетевой обмен с помощью TCP/IP [Электронный ресурс]. – http://www.citforum.ru/internet/comer/contents.shtml. (Дата обращения 15.03.1012)
4. Модель OSI [Электронный ресурс]. – http://www.citforum.ru/nets/switche/osi.shtml. (Дата обращения 15.03.1012)
5. Олифер, Н. А. Базовые технологии локальных сетей [Электронный ресурс] / Н. А. Олифер, В. Г. Олифер. – http://www.citforum.ru/nets/protocols2/index.shtml. (Дата обращения 15.03.1012)
6. Олифер, Н. А. Введение в IP-сети [Электронный ресурс] / Н. А. Олифер, В. Г. Олифер. – http://www.citforum.ru/nets/ip/contents.shtml. (Дата обращения 15.03.1012)
7. Олифер, Н. А. Роль коммуникационных протоколов и функциональное назначение основных типов оборудования корпоративных сетей [Электронный ресурс] / Н. А. Олифер, В. Г. Олифер. – http://www.citforum.ru/nets/protocols/index.shtml. (Дата обращения 15.03.1012)
8. Руководство по сетям Ethernet для начинающих [Электронный ресурс] . – http://www.citforum.ru/nets/ethernet/starter.shtml. (Дата обращения 15.03.1012)

Учебное издание

ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Учебное пособие

Составители: КАПУСТИН Дмитрий Александрович,
ДЕМЕНТЬЕВ Виталий Евгеньевич

ЛР № 026040 от 22.10.97.

Подписано в печать 27.12.2011. Формат 60×84 /16.
Усл. п. л. 8,37. Тираж 100 экз. Заказ 291.

Ульяновский государственный технический университет
432027, Ульяновск, Сев. Венец, 32

Типография УлГТУ. 432027, Ульяновск, Сев. Венец, 32