Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

В. П. ГАЛАС

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ, СЕТИ И ТЕЛЕКОММУНИКАЦИИ

УЧЕБНИК

В двух частях

Часть 2. Сети и телекоммуникации

Владимир 2017

УДК 658.512.011.56;004.91(021);621.372(075)
ББК 32.9
Г15

Рецензенты:

Кандидат технических наук, доцент
доцент кафедры вычислительной техники
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
В. Б. Буланкин

Кандидат технических наук
технический директор ООО «НПП ”Энергоприбор”»
С. А. Кокорин

Печатается по решению редакционно-издательского совета ВлГУ

Галас, В. П.

Г15 Вычислительные системы, сети и телекоммуникации : учебник. В 2 ч. Ч. 2. Сети и телекоммуникации / В. П. Галас ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2017. − 284 с. – ISBN 978-5-9984-0817-5 (ч. 2). – ISBN 978-5-9984-0731-4.

Вторая часть учебника включает девять глав. Излагаются принципы построения, архитектура, функциональная и структурная организация вычислительных сетей и телекоммуникаций. Рассматриваются функционирование, программное обеспечение и перспективы развития. Основная цель учебника – познакомить студентов и специалистов, профессиональная деятельность которых связана с использованием вычислительных сетей, с широким кругом вопросов, касающихся принципов построения и организации функционирования вычислительных систем, стандартами проектирования, режимами работы и предоставляемыми услугами сетей. Изложение учебника базируется на публикациях отечественных и зарубежных авторов, кроме теоретических основ в учебнике приводятся контрольные вопросы, требующие самостоятельного изучения материала и углубления знаний в области вычислительных сетей.

Учебник представляет собой издание с интерактивным вложением на компакт-диске. Диск содержит теоретический материал, разделенный на главы, включающие основной материал, контрольные вопросы, дополнительный справочный и интерактивный материалы, систему меню и гиперссылок, встроенные программы тестирования знаний, блок контрольных мероприятий с программами для реализации рейтинг-контроля в процессе обучения, а также все необходимые инструкции для работы с диском, кроме того, приведены списки библиографической и рекомендуемой литературы.

Предназначен для студентов направлений 09.03.03 – Прикладная информатика, 27.03.04 – Управление в технических системах, а также для студентов других направлений бакалавриата и слушателей всех форм обучения с использованием мультимедийных и дистанционных образовательных технологий, может быть полезен преподавателям высших и средних специальных учебных заведений.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Табл. 10. Ил. 103. Библиогр.: 36 назв.

УДК 658.512.011.56;004.91(021);621.372(075)
ББК 32.9

ISBN 978-5-9984-0817-5 (ч. 2)
ISBN 978-5-9984-0731-4

© ВлГУ, 2017

ОГЛАВЛЕНИЕ

Глава 10. НАЗНАЧЕНИЕ, РЕЖИМЫ РАБОТЫ И КЛАССИФИКАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ ПРИКЛАДНЫМИ ПРОЦЕССАМИ 9

10.1. Назначение вычислительных сетей. Основные определения и термины 9

10.2. Режимы работы и предоставляемые услуги 13

10.3. Классификация вычислительных сетей 14

10.4. Управление взаимодействием прикладных процессов 19

Вопросы к компьютерному тестированию 28

Глава 11. ТЕХНОЛОГИИ ВЫСОКОСКОРОСТНЫХ ГЛОБАЛЬНЫХ СЕТЕЙ 30

11.1. Общая характеристика 30

11.2. Сети и технологии *ISDN* 32

11.3. Сети и технологии *PDH* 37

11.4. Сети и технологии *SDH* 39

11.5. Сети и технологии *DWDM* 44

11.6. Сеть и технология *X*.25 46

11.7. Сеть и технология *Frame Relay* 49

11.8. Сеть и технология *ATM* 52

Вопросы к компьютерному тестированию 55

Глава 12. СРЕДСТВА ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ 57

12.1. Линии связи и каналы передачи данных 58

12.2. Техническое обеспечение информационно-вычислительных сетей 64

12.2.1. Серверы и рабочие станции 64

12.2.2. Концентраторы, приемопередатчики и повторители 69

12.2.3. Мосты, маршрутизаторы, коммутаторы и шлюзы 72

12.2.4. Модемы и факс-модемы 81
12.2.5. Сетевые адаптеры и анализаторы 85
12.3. Информационное обеспечение сети 89
12.4. Программное обеспечение сети 91
Вопросы к компьютерному тестированию 95

Глава 13. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ. УПРАВЛЕНИЕ ДОСТУПОМ, СТАНДАРТЫ ПРОЕКТИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ 98
13.1. Основные определения и преимущества 98
13.2. Классификация ЛВС 99
13.3. Основные характеристики и области применения ЛВС..... 103
13.4. Организация управления ЛВС 104
13.5. Методы доступа к передающей среде в локальных вычислительных сетях 109
13.6. Стандарты проектирования и использования сетей 112
Вопросы к компьютерному тестированию 118

Глава 14. СТЕКИ ПРОТОКОЛОВ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ ЛВС 120
14.1. Стеки протоколов верхнего и среднего уровней..... 121
14.1.1. Сетевые протоколы 121
14.1.2. Транспортные протоколы 122
14.1.3. Прикладные протоколы 122
14.1.4. Стек *OSI* для протоколов верхнего и среднего уровней 123
14.1.5. Архитектура стека протоколов *Microsoft TCP/IP*..... 123
14.1.6. Адресация в *IP*-сетях 129
14.1.7. Протоколы сопоставления адреса *ARP* и *RARP*..... 130
14.1.8. Протокол *ICMP* 131
14.1.9. Протокол *IGMP* 131
14.1.10. Протокол *NDIS* 131
14.1.11. Уровень сетевого интерфейса 132
14.2. Настройка *IP*-адресации и маршрутизации 132
14.2.1. Основы *IP*-адресации..... 132
14.2.2. Классовая и бесклассовая *IP*-адресация 134

14.2.3. IP-адреса для локальных сетей 136
14.2.4. Основы *IP*-маршрутизации 136
14.2.5. Назначение *IP*-адресов и проверка работоспособности *TCP/IP* 142
14.3. Протоколы передачи данных нижнего уровня 145
14.4. Определение основных характеристик системы передачи данных 156
Вопросы к компьютерному тестированию 160

Глава 15. ТОПОЛОГИИ И ТЕХНОЛОГИИ ПРОВОДНЫХ ЛВС 162
15.1. Сетевые топологии..... 162
15.1.1. Шинная топология 162
15.1.2. Топология типа «звезда» 163
15.1.3. Кольцевая топология 164
15.1.4 Комбинированные топологии ЛКС 165
15.2. Сетевые технологии 166
15.2.1. Технология *Ethernet* 166
15.2.2. *Fast Ethernet* 173
15.2.3. Стандарт *Gigabit Ethernet* 174
15.2.4. Технология *Token Ring* 175
15.2.5. Технология *ARCnet* 176
15.2.6. Технология *FDDI* 177
15.2.7. Домашние сети на базе электропроводки 179
Вопросы к компьютерному тестированию 182

Глава 16. БЕСПРОВОДНЫЕ ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ 184
16.1. Технология *Bluetooth* 184
16.2. Технология *GPRS* 186
16.3. Беспроводная передача данных по технологии *Wi-Fi* 187
16.4. Технология *MIMO* 190
16.5. Технология *Mesh* 191
16.6. Технология *WiMAX* 194
Вопросы к компьютерному тестированию 197

Глава 17. АКТУАЛЬНЫЕ И СТРУКТУРИРОВАННЫЕ ЛОКАЛЬНЫЕ И ПРОМЫШЛЕННЫЕ СЕТИ 199
17.1. Актуальные локальные вычислительные сети 199
17.1.1. Локальная вычислительная сеть *Novell Net Ware* 200
17.1.2. Локальные сети, управляемые операционной системой *Windows NT* 203
17.2. Структурированные ЛВС с использованием асимметричных *VLAN*-технологий 207
17.2.1. Виртуальная локальная сеть 207
17.2.2. Варианты использования асимметричных *VLAN* 209
17.3. Промышленные сети 215
17.3.1. Общие понятия и определение 215
17.3.2. Основные критерии выбора 219
17.3.3. Протоколы 220
Вопросы к компьютерному тестированию 233

Глава 18. ГЛОБАЛЬНАЯ СЕТЬ *INTERNET* 235
18.1. Введение в *Internet* 235
18.2. Работа со службами *Internet* 236
18.2.1. Терминальный режим 238
18.2.2. Электронная почта 239
18.2.3. Списки рассылки 239
18.2.4. Служба телеконференций 240
18.2.5. Служба *World Wide Web* 241
18.2.6. Служба имен доменов 244
18.2.7. Служба передачи файлов (*FTP*) 247
18.2.8. Служба *Internet Relay Chat* 248
18.2.9. Служба *ICQ* 248
18.2.10. Облачные технологии 249
18.3. Глобальная сеть *Internet*-2 254
Вопросы к компьютерному тестированию 261

ЗАКЛЮЧЕНИЕ 263

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ 265

ГЛОССАРИЙ 269

ВВЕДЕНИЕ

Вычислительные сети и телекоммуникации – значимая часть современного мира, а область их применения охватывает буквально все сферы человеческой деятельности.

Вычислительные сети создаются для эффективного предоставления различных информационно-вычислительных услуг пользователям сети в результате обеспечения быстрого и надежного доступа к аппаратным, программным и информационным ресурсам, распределенным в этой сети.

Так как связь между компонентами вычислительной сети может, как правило, осуществляться на больших расстояниях, в названии технических средств связи это подчеркивается наличием приставки «теле» (на расстоянии), то есть телекоммуникационные средства, или просто телекоммуникации.

Всемирная тенденция к объединению компьютеров в сети обусловлена рядом важных причин, таких как ускорение передачи информационных сообщений, возможность быстрого обмена информацией между пользователями, получение и передача сообщений, не отходя от рабочего места, возможность мгновенного получения любой информации из любой точки земного шара, а также обмен информацией между компьютерами разных фирм и производителей, работающих под разным программным обеспечением.

Последние два десятилетия характеризуются динамичным развитием сетевых технологий. Это связано с интенсивным внедрением веб-технологий, электронной почты, потокового аудио и видео, систем обмена сообщениями в реальном времени и т. п. Повсеместное использование компьютерных сетей требует от современного пользователя наличия соответствующих знаний и навыков. Важное значение в приобретении этих знаний имеет раздел «Сети и телекоммуникации» общего учебного курса дисциплины «Вычислительные системы, сети и телекоммуникации». Сам учебный предмет, включающий в себя множество сетевых концепций и технологий, является достаточно сложным для освоения. Кроме того, профессиональная литература, целиком посвященная компьютерным сетям, слишком избыточна и сложна для понимания студентами непрофильных

специальностей и направлений, а также не совсем удобна преподавателям при подготовке к занятиям в рамках курсов, содержащих только краткую информацию по компьютерным сетям.

Вопросы технической реализации компонентов вычислительных сетей в доступной форме рассмотрены в 1-й части учебника «Вычислительные системы, сети и телекоммуникации». Вторая часть учебника включает девять глав, в которых предпринята попытка компактного изложения основ технологий компьютерных сетей и телекоммуникаций без углубления в детали, объяснения общеупотребительных в настоящее время терминов и определений, связанных с функционированием компьютерных сетей.

Порядок изложения материала в пособии следующий: вначале приводятся наиболее важные термины и определения, назначение и классификация вычислительных сетей, принципы управления взаимодействием прикладными процессами, далее дается общее описание сетевых компьютерных топологий и технологий, рассматриваются основные средства обеспечения функционирования вычислительных сетей, аппаратное обеспечение *IP*-сетей, сетевые телекоммуникации, принципы адресации, протоколы, службы, отвечающие за сетевой обмен информацией и диагностику в вычислительных сетях. Кроме этого приводится стек протоколов *TCP/IP* как самый широко используемый, даются основы построения и функционирования беспроводных, актуальных и структурированных локальных и промышленных сетей, глобальных компьютерных сетей, популярных сетевых служб и сервисов, таких как Всемирная паутина *WWW*, служба передачи файлов *FTP*, электронная почта, служба трансляции имен и облачные сервисы. В довершение с целью закрепления изложенного в учебнике материала даны контрольные вопросы в форме, позволяющей проводить компьютерное тестирование. В учебнике также приводятся список рекомендуемой литературы и глоссарий.

Обе части электронного учебника содержат интерактивные вложения на компакт-дисках. Диски, в свою очередь, предлагают для изучения теоретический материал, разделенный на отдельные главы с вопросами для самопроверки, содержат систему меню и гиперссылок, электронную книгу с эффектом перелистывания страниц и тематическим поиском, глоссарий, список рекомендуемой литературы, дополнительный справочный и видеоматериал, встроенные программы тестирования знаний, блок контрольных мероприятий с программами для реализации тестирования в процессе обучения, а также все необходимые инструкции для работы с диском.

Глава 10

НАЗНАЧЕНИЕ, РЕЖИМЫ РАБОТЫ И КЛАССИФИКАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ ПРИКЛАДНЫМИ ПРОЦЕССАМИ

Рассматриваемые вопросы:

10.1. Назначение вычислительных сетей.
Основные определения и термины.
10.2. Режимы работы и предоставляемые услуги.
10.3. Классификация вычислительных сетей.
10.4. Управление взаимодействием прикладными процессами.

10.1. Назначение вычислительных сетей. Основные определения и термины

По мере развития и увеличения объемов баз данных, усложнения средств программного обеспечения, в том числе и прикладного, возникла насущная необходимость в соединении отдельных компьютеров между собой. Такое связывание компьютеров, позволяющее объединить их ресурсы – процессоры, память (внутреннюю и внешнюю, включая жесткие диски, разнообразные внешние устройства – принтеры, факс-аппараты, модемы и др.), каналы связи, и представляет собой вычислительную сеть, в которой каждый компьютер может передать другому компьютеру, подключенному к сети, любой набор данных.

Таким образом, любая компьютерная система, состоящая из нескольких компьютеров, наверняка перерастет в более сложную систему, которая потребует высокоскоростного обмена данными между компьютерами с сервисными возможностями. Такой обмен не может быть организован при помощи стандартных простых средств операционных систем (ОС) и прикладных программ, а требует организации принципиально новой информационной структуры – вычислительной сети.

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.

Различают два понятия сети: *коммуникационная сеть* и *информационная сеть*.

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

Прием и передачу звука, сигнала, текста, знака, письменного изображения по кабельной, проводной, магнитной, оптической, радио- и другим сетям принято называть телекоммуникацией.

Телекоммуникация (telecommunication) – форма связи, способ передачи информации на большие расстояния.

Система технических средств, с помощью которой осуществляется телекоммуникация, называется *сетью телекоммуникаций*.

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, или объект, способный осуществлять хранение, обработку или передачу информации. 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.

Компьютерная сеть (КС) состоит из *информационных систем* и *каналов связи* и представляет собой магистральные информационные структуры, состоящие из физического и логического уровней или составляющих, основное назначение которых – обмен информацией.

Физический уровень представлен компонентами сети, обеспечивающими физическое соединение между компьютерами (рис. 10.1). Такими компонентами, как правило, являются *сетевой интерфейс* (сетевая карта, или плата сетевого адаптера, стандартный или расширенный коммуникационный, или параллельный порты), *сетевая среда* передачи данных (кабель коаксиальный, двухпроводный (витая пара) или оптоволоконный) и *узловые элементы* (маршрутизаторы, концентраторы, повторители (репитеры, хабы (*hub*)), переключатели (*switch*)) и *конечные элементы* (терминаторы, коннекторы, разъемы, заглушки).

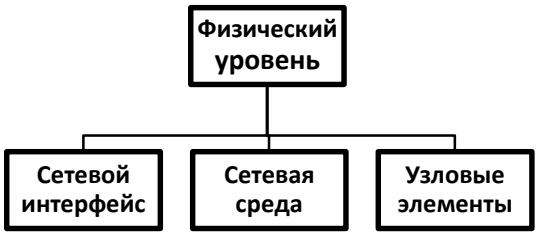


Рис. 10.1. Схема физического уровня сети

Логический уровень – это разнообразное программное обеспечение, предоставляющее возможность использования имеющихся в наличии физических компонент сети (рис. 10.2). Среди всего многообразия ПО можно выделить несколько типов: *драйверы* и *демон-процессы* сетевых протоколов операционных систем, *программы-серверы* и *клиенты* сетевых сервисов или служб.

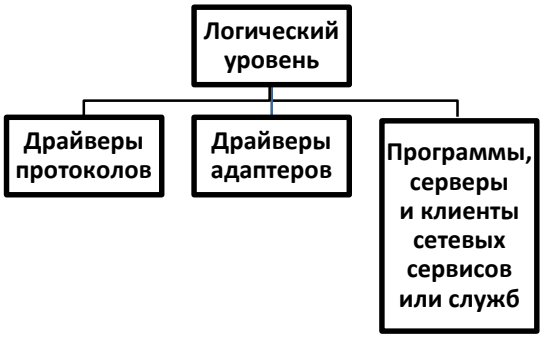


Рис. 10.2. Схема логического уровня сети

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, который прокладывается по маршруту в одном или нескольких физических каналах, его 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 собой 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 организации 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: 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. Все эти понятия будут рассмотрены более подробно при дальнейшем изучении.

10.2. Режимы работы и предоставляемые услуги

Режимы работы:

- обмен данными между абонентскими системами;
- запрос и выдача информации;
- сбор данных;
- пакетная обработка по запросам удаленных пользователей;
- диалоговый режим.

Предоставляемые услуги:

- телекоммуникационные услуги – электронная почта, телеконференции и телесеминары, электронные доски объявлений, передача больших массивов – файлов, размножение сообщений и передача их по заранее подготовленному списку и др.;
- информационные услуги – поиск информации по вопросам, интересующим абонентов;
- консультационные услуги – консультации по информационному и программному обеспечению сети, консультации по технологии использования общесетевых ресурсов и др.;
- технические услуги – установка программного обеспечения, установка и тестирование модемов и др.;
- рекламные услуги – размещение рекламы в электронных конференциях и семинарах, на электронных досках объявлений.

10.3. Классификация вычислительных сетей

Классификация вычислительных сетей производится по следующим принципам (рис. 10.3):

Рис. 10.3. Классификация компьютерных сетей

1. По функциональному принципу:

• вычислительные сети – сети, ориентированные на обработку данных, большая часть работ связана с вычислительными процедурами;

• информационные сети – преобладающим является информационно-справочная работа.

2. *По информационному принципу* сети в зависимости от организации передачи делят на несколько групп:

• сети с селекцией информации – информация как бы вбрасывается в сеть вся, но извлечь ее может только тот абонентский пункт, которому она предназначена;

• сети с маршрутизацией информации – устанавливается маршрут от источника к получателю, и информация идет только по этому маршруту. Информация, таким образом, доступна только получателю.

Сети с маршрутизацией, в свою очередь, делятся на три группы:

• сети с коммутацией каналов;

• сети с коммутацией сообщений;

• сети с коммутацией пакетов.

3. *По принципу структурной классификации* сети делят на абонентские (АбС) и ассоциативные (АсС) системы (рис. 10.4).

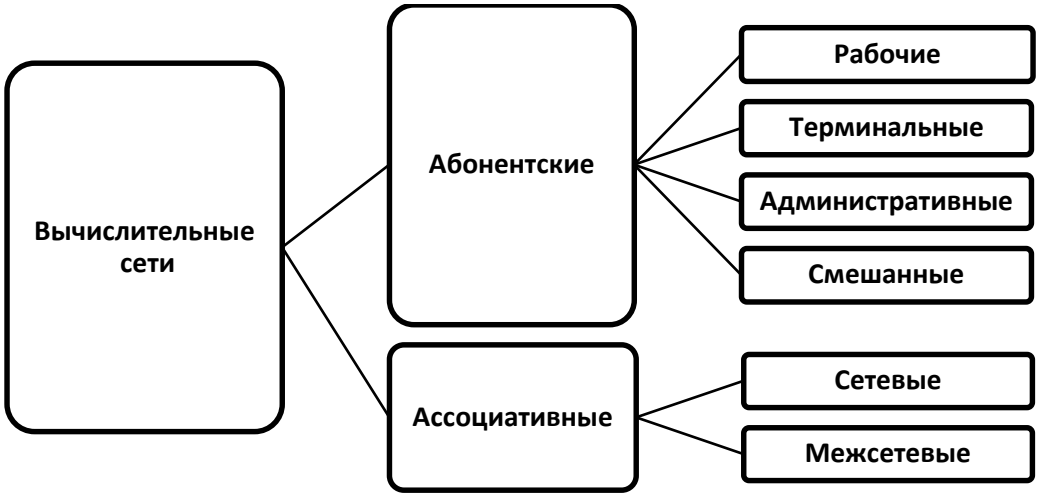


Рис. 10.4. Структурная классификация сети

Абонентские системы в зависимости от выполняемых функций подразделяются на четыре вида: рабочие, терминальные, административные и смешанные.

Рабочая система предназначена для предоставления пользователю информационно-вычислительных ресурсов: банка данных, результатов обработки задач по подсистемам АСУ и т.д.

Терминальная система предоставляет абонентам (пользователям) информационно-вычислительной системы (ИВС) через один или

несколько терминалов информационно-вычислительные ресурсы рабочих систем (часто функции рабочей и терминальной систем совмещены).

Административной называется система, на которую возлагаются функции управления всей либо какой-нибудь частью ИВС.

Смешанной система называется в том случае, если она выполняет функции двух, а иногда даже трёх рассмотренных выше видов абонентских систем.

Ассоциативные системы в зависимости от выполняемых функций подразделяются на два вида: межсетевые и сетевые.

Межсетевой называется ассоциативная система, предназначенная для обеспечения взаимодействия двух либо более ИВС.

Ассоциативная система, которая связывает абонентские системы внутри одной сети, получила название *сетевой*.

4. *По территориальному признаку*

Основным признаком отличия является классификация КС по размерам.

В зависимости от протяжённости КС принято делить на три вида: локальные, региональные и глобальные (рис. 10.5).

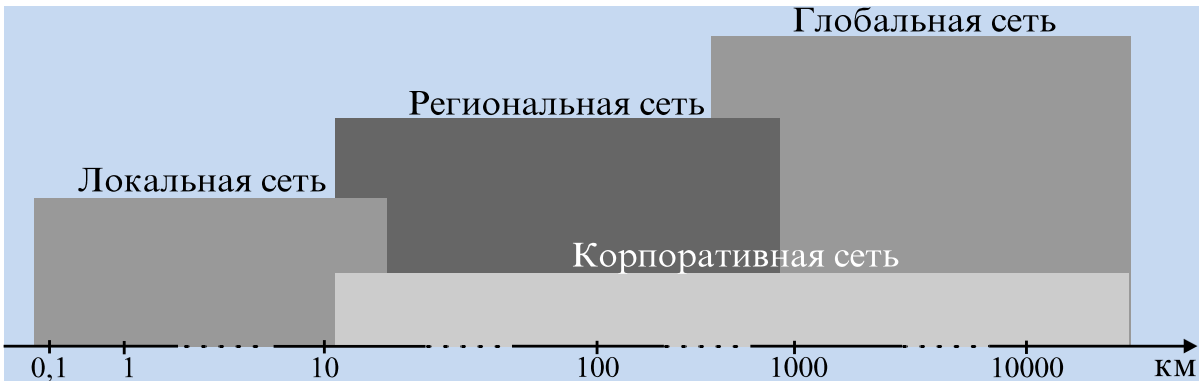


Рис. 10.5. Классификация сетей по территориальному признаку

Локальной называется сеть, абоненты которой находятся на небольшом расстоянии друг от друга. Протяженность локальной компьютерной сети (ЛКС) ограничивается несколькими километрами. Обычно ЛКС охватывают одно либо несколько расположенных рядом зданий. Именно на базе локальной ИВС разрабатываются современные АСУ фирмы, банка, вуза и т.д.

Региональная компьютерная сеть (РКС) связывает абонентов, расположенных на значительном (от 10 до 1000 км) расстоянии друг от друга. Она может включать абонентов района, города, области и даже небольшой страны.

Глобальная компьютерная сеть (ГКС) является третьим видом ИВС, она объединяет абонентов, расположенных на территории большой страны, разных стран и даже континентов. Построение этой сети возможно с помощью спутников. В настоящий момент имеется несколько глобальных компьютерных сетей и их протоколов, например, *RelCom, CompuServ, Internet* и т.д. Большинство таких сетей имеют тысячи серверов, десятки и сотни тысяч пользователей и носят статус международных, так как связывают компьютерные системы различных стран и континентов.

В последнее время для характеристики ИВС всё чаще стали использовать понятие *корпоративные* компьютерные сети (ККС). Эти сети объединяют ряд предприятий одной фирмы, в зависимости от взаиморасположения предприятий они могут быть региональными или глобальными. АС в таких сетях взаимодействуют на базе различных территориальных сетей связи, в которых используются телефонные линии связи, радиосвязь, системы спутниковой связи. ККС – техническая база корпорации. Им принадлежит ведущая роль в реализации задач планирования, организации и осуществления производственно-хозяйственной деятельности корпорации.

5. По условиям доступа

Все сети, в том числе и глобальные, делят на *коммерческие,* в которых доступ и услуги сервисных служб платные, и *некоммерческие* – т.е. «условно бесплатные». Условно означает, что какую-то плату за подключение и использование сетевых служб, а также эксплуатацию систем связи пользователь все-таки вносит, но она несоизмеримо меньше, нежели в коммерческих системах, однако и уровень сервиса соответственный.

Коммерческие сети поддерживаются профессиональными организациями, цель которых – предоставление сетевых услуг и высококачественного коммерческого сетевого сервиса.

Некоммерческие, как правило, поддерживаются на добровольных началах образовательными и информационными структурами и

организациями общественного характера, не имеют четкой организации, единого управления, целенаправленного структурирования и стратегии развития.

6. *По топологии* сети делятся:

• на широковещательные – сети, в которых информация передается сразу по всей сети (сети с селекцией информации);

• сети с последовательной передачей – когда информация либо напрямую отправляется получателю, либо проходит несколько последовательных сегментов сети и доступна только конкретному получателю.

К широковещательным структурам относятся общая шина, «звезда» с пассивным центром, дерево (рис. 10.6).

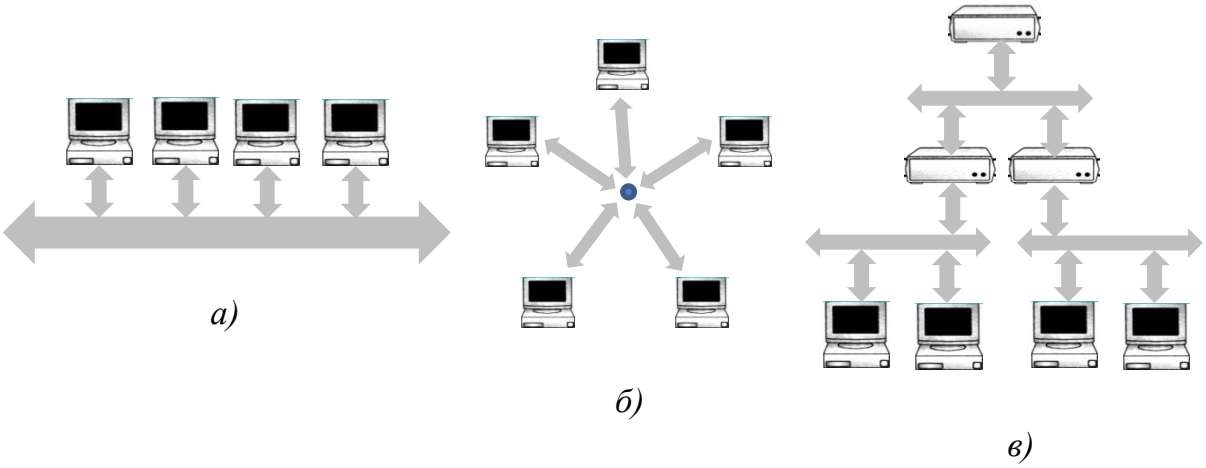


Рис. 10.6. Широковещательные конфигурации сетей:
а – общая шина; *б* – «звезда» с пассивным центром; *в* – дерево

В таких структурах в каждый момент времени активна одна станция. Сообщения доступны всем, но принимает их только та, которой они предназначены.

В последовательных конфигурациях, характерных для сетей с маршрутизацией информации, данные передаются последовательно от одной РС к соседней, причем на различных участках сети могут использоваться разные виды физической передающей среды.

К последовательным конфигурациям относятся произвольная (ячеистая), полносвязная, «кольцо», «цепочка», «звезда» с интеллектуальным центром (рис. 10.7).

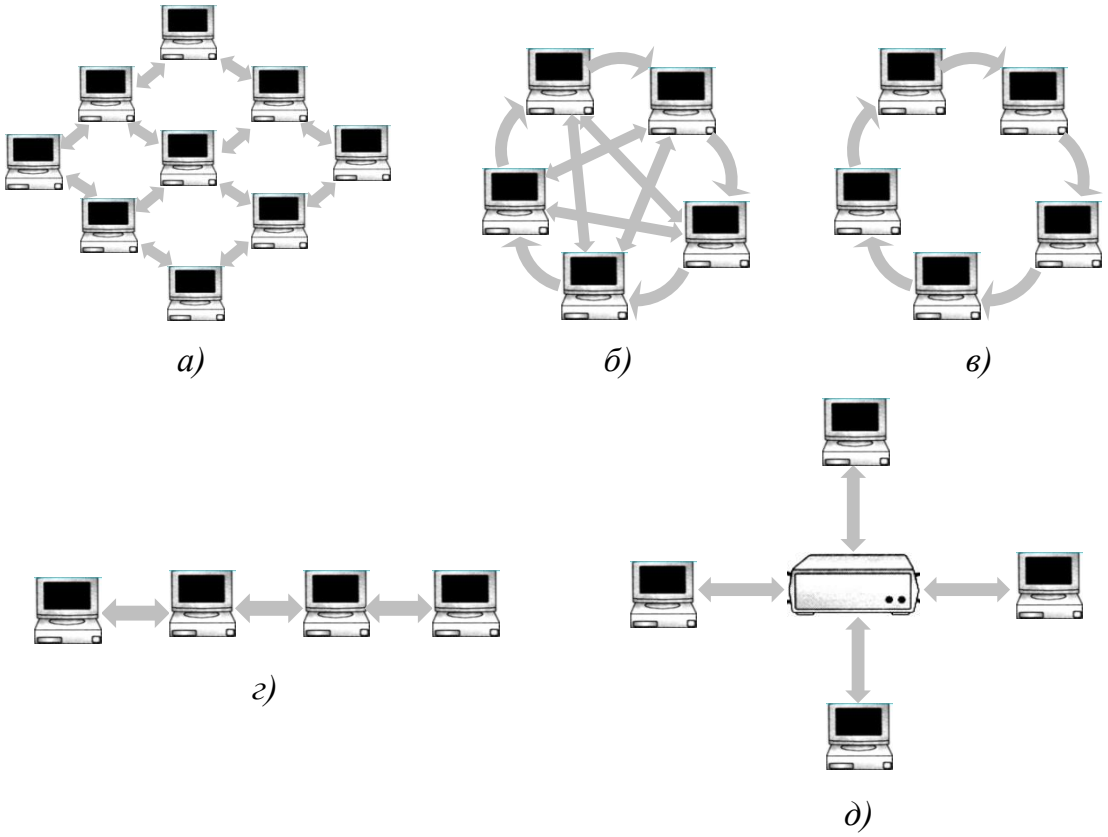


Рис. 10.7 – Последовательные конфигурации сетей:
а – ячеистая, *б* – полносвязная, *в* – «кольцо»; *г* – «цепочка»;
д – «звезда» с интеллектуальным центром

7. *По виду обмена*

Все сети делятся еще на четыре группы в зависимости от того, как организована передача по одному и тому же каналу в различных направлениях:

1) *симплексные сети* – обмен происходит так: от А до В один канал, а от В к А – другой;

2) *полудуплексные сети* – в момент времени t_1 – передача от А к В, а в момент t_2 – наоборот;

3) *дуплексные сети* – передача в обе стороны может осуществляться одновременно;

4) *широкополосные системы* – с применением различной несущей частоты для одновременной передачи сигналов в двух направлениях.

10.4. Управление взаимодействием прикладных процессов

В современных вычислительных сетях это управление строится по двум принципам:

1) связь между процессами без участия функциональной среды;

2) связь между прикладными процессами только через функциональную среду.

В первом случае – организация взаимодействия между прикладными процессами выполняется только с помощью единой сетевой операционной системы (СОС). Главный недостаток – чрезмерно высокая сложность СОС и как следствие – невысокая надежность.

Связь через функциональную среду в своей основе имеет следующий подход – все, что нужно выполнить в сети для организации взаимодействия прикладных процессов, разбивают на определенный набор функций, причем эти функции образуют иерархическую многоуровневую структуру (нижние этажи обслуживают верхние, а те – управляют нижними). Каждый уровень решает свою задачу, и управление в значительной мере упрощается. Обязательно условие – в этой системе должен быть предусмотрен стандартный набор правил, который реализуется на каждом уровне. Этот набор называют уровневым протоколом.

Международная организация по стандартам (*International Standards Organization* (*ISO*)) разработала модель, которая четко определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень. Эта модель называется моделью взаимодействия открытых систем (*Open System Interconnection* (*OSI*)) или моделью *ISO/OSI*.

Это обязательный стандарт для работающих в сетевой области. В основу его положена семиуровневая эталонная модель взаимодействия открытых систем (ВОС) (рис. 10.8).

Сетевая модель *OSI* была введена *ISO* в целях стандартизации построения сетевых протоколов взаимодействия открытых систем и состоит из семи уровней.

1. ***Физический уровень*** – здесь решаются вопросы организации физического пути для передаваемых сигналов.

На этом уровне устанавливается, поддерживается и расторгается соединение с физическим каналом, определяются электрические и функциональные параметры взаимодействия ЭВМ с коммуникационной подсетью.

Уровень имеет дело с передачей битов по физическим каналам, таким, например, как коаксиальный кабель, витая пара или оптоволоконный кабель. К этому уровню имеют отношение характеристики физических сред передачи данных – полоса пропускания, помехозащищенность, волновое сопротивление и др. На этом же уровне определяются характеристики электрических сигналов, такие как требования к фронтам импульсов, уровням напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого здесь стандартизуются типы разъемов и назначение каждого контакта.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

АС-1		АС-*N*
Прикладные процессы	**Уровневые протоколы**	**Прикладные процессы**
7. Прикладной	пользовательское управление данными	7. Прикладной
6. Представительный	интерпретация передаваемых данных	6. Представительный
5. Сеансовый	поддержка диалога между удаленными процессами	5. Сеансовый
4. Транспортный	обеспечение взаимодействия удаленных процессов	4. Транспортный
3. Сетевой	маршрутизация, управление потоками данных	3. Сетевой
2. Канальный	формирование кадров, управление доступом к среде	2. Канальный
1. Физический	битовые протоколы передачи информации	1. Физический
Передающая среда (коммуникационная подсеть)		

Рис. 10.8. Семиуровневая эталонная модель взаимодействия открытых систем

Примером протокола физического уровня может служить спецификация 10*Base-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 м, манчестерский код для представления данных на кабеле и другие характеристики среды и электрических сигналов.

2. ***Канальный уровень*** – здесь определяются правила использования физических каналов абонентскими станциями. Сюда входит организация каналов связи, управление ими, защита от ошибок и других операций. На канальном уровне при помощи специальной аппаратуры на одной и той же физической линии связи создают несколько каналов связи, а поскольку прокладка линий связи – 40 % от стоимости, то это существенно.

Одна из задач канального уровня – проверка доступности среды передачи. Другая задача канального уровня – реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (*frames*). 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.

К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, «кольцо» и «звезда». Примерами протоколов канального уровня являются протоколы *Ethernet, Token Ring, FDDI,* 100*VG-AnyLAN*.

3. ***Сетевой уровень***, на котором решаются две основные задачи – буферизация и маршрутизация. Задача маршрутизации заключается в прокладывании маршрута между двумя абонентскими станциями, взаимодействующими в данный момент времени. Он определяется состоянием сети. На сетевом уровне происходит организация логических каналов – совокупностей всей аппаратуры, необходимой для прокладывания маршрута, и программных средств. Логический канал должен быть организован так, чтобы у взаимодействующих абонентских станций было представление о том, что они являются единственными поль-

зователями физического канала. Буферизация – процесс согласования объема и скоростей передачи информации с параметрами конкретных участков сети. Каждый фрагмент маршрута имеет свои показатели: объем и скорость передачи, их и нужно согласовывать.

Сообщения сетевого уровня принято называть *пакетами (packets)*. 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.

На сетевом уровне определяются 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. К сетевому уровню относят и другой вид протоколов – *протоколы 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.

Примерами протоколов сетевого уровня являются протокол межсетевого взаимодействия *IP* стека *TCP/IP* и протокол межсетевого обмена пакетами *IPX* стека *Novell*.

4. ***Транспортный уровень*** – действительно центральный уровень; отделяет пользователей сети от функционального и физического уровней, т.е. от нижних уровней сетевой модели. Благодаря ему пользователю совершенно не обязательно знать то, что происходит на нижнем уровне. Обеспечивается связь между коммуникационной подсетью и верхними уровнями рассматриваемой модели. Основная задача данного уровня – управление потоком данных пользователя (управление трафиком). В настоящее время в связи с тем что основным способом коммутации в сетях является коммутация пакетов, на транспортном уровне выполняется деление сообщений на пакеты, а затем в точке приема – формирование из них исходных сообщений (восстановление из пакетов исходного сообщения). Ниже транспортного уровня основная информационная единица – пакет данных, выше – сообщение.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети – компонентами их сетевых операционных систем. В качестве примера

транспортных протоколов можно привести протоколы *TCP* и *UDP* стека *TCP/IP* и протокол *SPX* стека *Novell*.

5. ***Сеансовый уровень*** – это организация и управление сеансами взаимодействия прикладных процессов. Сеансы организуются по запросам пользователей, которые поступают через прикладной и представительный уровни. На сеансовом уровне выполняются управление очередностью передачи данных, затем синхронизация отдельных событий и выбор формы диалога пользователей (либо дуплекс, либо полудуплекс).

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон активна 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 с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

6. ***Представительный уровень*** – здесь решаются задачи представления данных. Данные, поступающие на этот уровень с сеансового, преобразуются в форму, удобную для представления на дисплее. Выше представительского уровня сообщения получают уже явно смысловое выражение. Ниже этого уровня сообщения присутствуют в виде формальных кодов и смысл в явном виде отсутствует.

Этот уровень гарантирует то, что информация, передаваемая прикладным уровнем, будет понятна ему в другой системе. При необходимости уровень представления выполняет преобразование форматов данных в некоторый общий формат представления, а на приеме соответственно выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например синтаксические различия в представлении данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Пример протокола, работающего на уровне представления, – протокол *Secure Socket Layer (SSL)*, который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека *TCP/IP*.

7. ***Прикладной уровень*** – здесь обеспечивается поддержка прикладных пользовательских процессов. Это тоже своего рода граница, отделяющая прикладной пользовательский процесс от процессов, происходящих в сети.

Прикладной уровень – это в действительности просто 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. Единица данных, которой оперирует прикладной уровень, обычно называется *сообщением* (*message*).

Существует очень большое разнообразие протоколов прикладного уровня. Приведем в качестве примеров хотя бы несколько наиболее распространенных реализаций файловых сервисов: *NCP* в операционной системе *Novell NetWare*, *SMB* в *Microsoft Windows NT*, *NFS*, *FTP* и *TFTP*, входящие в стек *TCP/IP*.

Каждый из перечисленных уровней поддерживает интерфейсы с выше- и нижележащими уровнями (рис. 10.9).

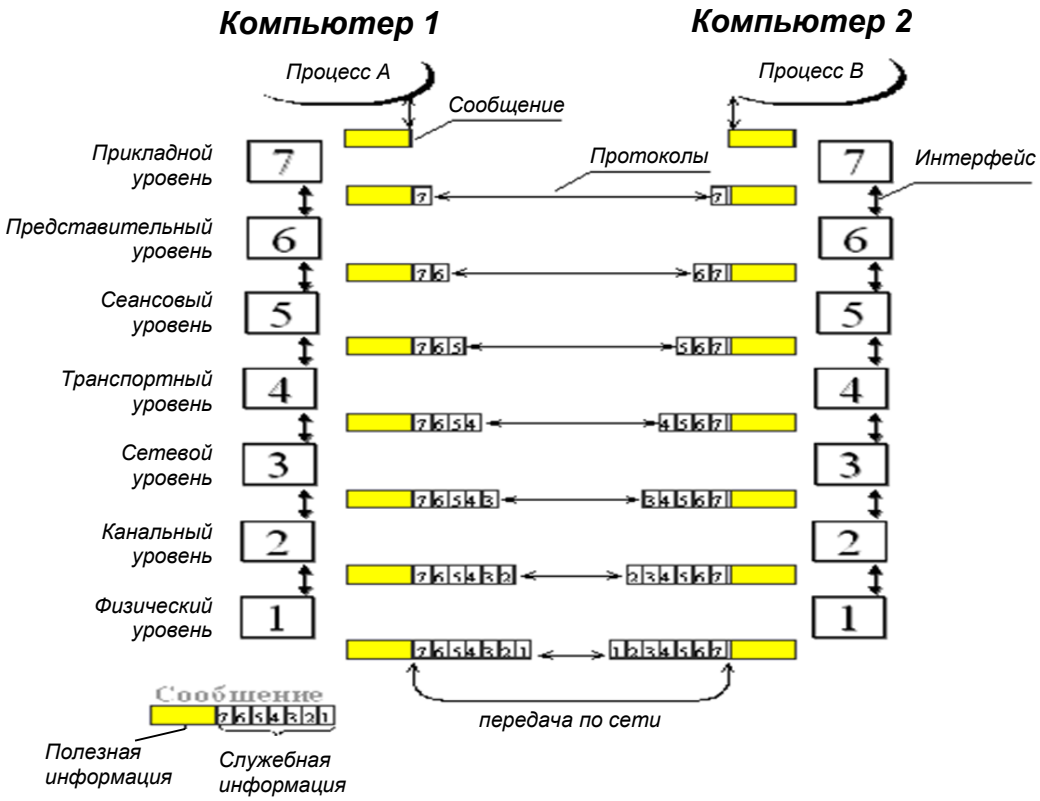


Рис. 10.9. Уровневое взаимодействие в сети

На основании запроса абонента сети программное обеспечение прикладного уровня формирует сообщение стандартного формата, в которое помещает служебную информацию (заголовок) и, возможно, передаваемые данные. Затем это сообщение направляется представительному уровню.

Представительный уровень добавляет к сообщению свой заголовок и передает результат вниз сеансовому уровню, который в свою очередь добавляет свой заголовок и т.д.

Наконец, сообщение достигает самого низкого, физического уровня, который действительно передает его по линиям связи.

Когда сообщение по сети поступает на другую машину, оно последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует, обрабатывает и удаляет заголовок своего уровня, выполняет соответствующие данному уровню функции и передает сообщение вышележащему уровню.

Все это очень похоже на работу почты. Лист бумаги с текстом отправителя передается с верхнего уровня вниз, проходя множество стадий. При этом он «обрастает» служебной информацией (конверт, адрес на конверте, почтовый индекс) и подвергается определенной обработке (почтальон в отделении забирает письмо, на конверт наклеивают марки, ставят штемпели, а после сортировки письмо попадает в контейнер для перевозки почты в другой город). Так информация отправителя доходит до самого нижнего уровня – почтового транспорта, которым она перевозится в пункт назначения. Там происходит обратный процесс: открывается контейнер, письмо извлекается, считывается адрес, после чего почтальон доставляет письмо. А затем адресат получает информацию в первоначальном виде – когда извлекает лист из конверта, проверяет подпись и читает текст.

Помимо того что каждый уровень решает свои задачи, между уровнями существует определенное различие в средствах их реализации. Уровни 7 – 3 – программные средства (*Soft*); 4 – 1 – программные и аппаратные средства (*Hard&Soft*); 3 – 4 – аппаратные и программные с преобладанием последних; 2 – 1 – программные и аппаратные с преобладанием последних; 7 – 5 – уровни сетевого сервиса и т.д.

На нижних уровнях требования стандартов очень жесткие.

Функции всех уровней модели *OSI* могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня (физический, канальный и сетевой) – сетезависимые, т. е. протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием. Например, переход на оборудование *FDDI* означает полную смену протоколов физического и канального уровней во всех узлах сети.

Три верхних уровня – сеансовый, уровень представления и прикладной – ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от *Ethernet* на высокоскоростные технологии глобальных сетей не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

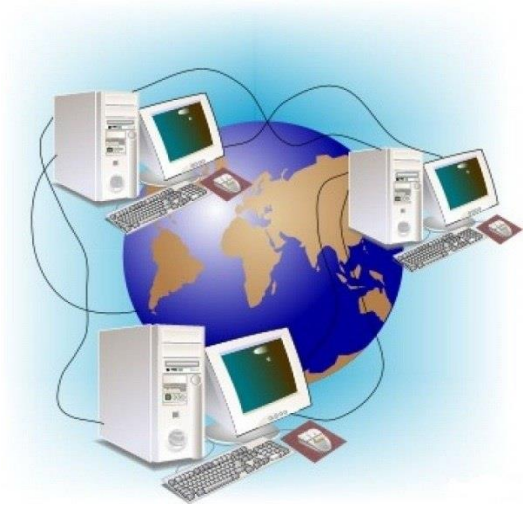
Транспортный уровень – промежуточный, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств, непосредственно занимающихся транспортировкой сообщений.

Компьютер с установленной на нем сетевой ОС взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост и коммутатор), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор).

Вопросы к компьютерному тестированию

1. Каково основное назначение компьютерной сети?
2. Привести название уровней информационной структуры компьютерной сети.
3. К какому уровню информационной структуры компьютерной сети относят сетевой интерфейс?
4. К какому уровню информационной структуры компьютерной сети относят драйверы?
5. Перечислить основные режимы работы компьютерных сетей.
6. Какие основные услуги предоставляют современные сети?
7. По каким принципам классифицируют компьютерные сети?
8. Какие компьютерные сети ориентированы на обработку данных?
9. В каких сетях преобладающим является информационно-справочная работа?
10. Какие компьютерные сети связывают абонентские системы, расположенные в пределах небольшой территории?
11. Какие компьютерные сети связывают абонентские системы, расположенные в пределах отдельной страны?
12. Какие компьютерные сети связывают абонентские системы, осуществляющие взаимодействие на базе различных территориальных сетей связи?
13. Какие компьютерные сети предназначены для реализации задач планирования, организации и осуществления производственно-хозяйственной деятельности?
14. На какие виды подразделяют сети при классификации их по топологии?
15. Какие структуры относят к широковещательным сетям?
16. Какие функции выполняет центральная станция в конфигурации «звезда с пассивным центром»?
17. В какой конфигурации компьютерных сетей на различных участках сети могут использоваться разные виды физической передающей среды?
18. В каких сетях двухсторонний одновременный обмен производится по двум каналам?

19. В каких сетях двухсторонний одновременный обмен производится по одному каналу?
20. В каких сетях двухсторонний обмен производится по одному каналу, но в разные промежутки времени?
21. Назовите семь уровней эталонной модели взаимодействия открытых систем.
22. Какой из уровней семиуровневой эталонной модели взаимодействия открытых систем занимает верхний этаж иерархической многоуровневой структуры?
23. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем осуществляются установление, поддержка и расторжение соединения с физическим каналом?
24. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем осуществляются организация каналов связи, управление ими, защита от ошибок?
25. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем решаются задачи буферизации и маршрутизации?
26. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем осуществляется управление потоком данных (трафиком) пользователя?
27. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем выполняется управление очередностью передачи данных?
28. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем осуществляется преобразование данных в форму, удобную для вывода на дисплей?
29. На каком из уровней семиуровневой эталонной модели взаимодействия открытых систем обеспечивается поддержка пользовательских процессов?
30. На каких уровнях семиуровневой эталонной модели взаимодействия открытых систем требования стандартов наиболее жесткие?



Глава 11

ТЕХНОЛОГИИ ВЫСОКОСКОРОСТНЫХ ГЛОБАЛЬНЫХ СЕТЕЙ

Рассматриваемые вопросы:

11.1. Общая характеристика.
11.2. Сети и технологии *ISDN*.
11.3. Сети и технологии *PDH*.
11.4. Сети и технологии *SDH*.
11.5. Сети и технологии *DWDM*.
11.6. Сеть и технология *X*.25.
11.7. Сеть и технология *Frame Relay*.
11.8. Сеть и технология *ATM*.

11.1. Общая характеристика

Высокоскоростная передача информации в глобальных (территориальных и корпоративных) сетях основана на ряде технологий, различных по принципу организации, быстродействию и используемой физической среде передачи информации.

Первой попыткой стандартизировать абонентские услуги, интерфейсы пользователь/сеть, сетевые и межсетевые возможности является создание *цифровой сети с интеграцией услуг ISDN (Integrated Serviced Digital Network),* которая использует обычные двухпроводные линии связи с мультиплексированием одного канала между несколькими абонентами.

Создание коммутируемой инфраструктуры, позволяющей быстро и гибко организовать постоянный канал с двухточечной топологией между двумя устройствами, подключенными к сети, было осуществлено с помощью ряда технологий *первичных (опорных) сетей связи*.

К ним относят три поколения технологий:

1. *Плезиохронная цифровая иерархия* (*Plesiochronous Digital Hierarchy, PDH*).

2. *Синхронная цифровая иерархия* (*Synchronous Digital Hierarchy, SDH* – Европа), в США – *SONET*.

3. *Уплотненное волновое мультиплексирование* (*DWDM*).

Первичная сеть связи – сеть стандартных каналов связи, обеспечивающая передачу информации в наиболее общей форме между ее пользователями.

На основе каналов, образованных первичными сетями, работают *вторичные* (*наложенные)* компьютерные и телефонные сети. Вторичная сеть связи – сеть каналов передачи определенного вида информации с использованием на физическом уровне каналов первичной сети связи.

Первые три технологии (*ISDN, PDH* и *SDH*) для разделения высокоскоростного канала используют *временное мультиплексирование* (*TDM*) и передают данные в цифровой форме.

Сети *PDH* и *SDH* поддерживают *иерархию скоростей*, так что пользователь может выбрать подходящую ему скорость для каналов, с помощью которых он будет строить сеть.

Технология *SDH* обеспечивает более высокие скорости, так что при построении крупной первичной сети ее магистраль строится на технологии *SDH*, а сеть доступа – на *PDH*.

Сети *DWDM* представляют собой последнее достижение в области создания высокоскоростных каналов. Они уже не являются цифровыми, так как предоставляют своим пользователям *выделенную волну* для передачи информации, которую можно задействовать по усмотрению – модулировать или кодировать. Технология *DWDM* вытесняет *SDH* из протяжённых магистралей на периферию сети, превращая ее в технологию сетей доступа.

Эти три различные технологии позволяют создать гибкую и масштабируемую первичную сеть, способную обслуживать большое количество компьютерных и телефонных сетей.

Технологии *X*.25, *Frame Relay* и *ATM* значительно отличаются от предыдущих по функциональным характеристикам. В то же время все они используют технику *виртуальных каналов*, которая является разновидностью техники, ориентированной на установление соединения.

Технология X.25 появилась на заре эры компьютерных сетей практически одновременно с сетью *ARPANET*, давшей начало *Internet* и дейтаграммному протоколу *IP*. В сетях *X*.25 виртуальные каналы используются для надежной передачи данных, что в 1970 – 80 гг., когда эта технология была очень популярна, было весьма актуально, так как многие линии связи были аналоговыми и не могли сами по себе обеспечить надежную передачу цифровых данных. Поэтому так ценилась способность *X*.25 к восстановлению искаженных и потерянных пакетов.

Особенность *технологии Frame Relay* (*FR*) состоит в том, что, освободившись от многих ненужных в современном телекоммуникационном мире функций, она выполняет только тот минимум, который необходим для доставки кадров адресату. Вместе с тем перечень возможностей *Frame Relay* был расширен за счет функции поддержки параметров качества обслуживания. В сетях *FR* возможна передача голоса с высоким качеством – для этого коммутаторы сети должны обеспечивать приоритезацию трафика.

Технология ATM предоставляет своим пользователям разнообразный и интегрированный набор транспортных услуг. В отличие от *X*.25 и *FR ATM* была изначально задумана как технология, ориентированная на передачу трафика всех существующих типов: компьютерных данных, голоса, видео, управления объектами и т. п. Фиксированный небольшой размер кадра позволяет минимизировать задержки трафика реального времени.

Рассмотрим упомянутые сети и технологии более подробно.

11.2. Сети и технологии *ISDN*

Цифровая сеть с интеграцией услуг *ISDN* (*Integrated Serviced Digital Network*) относится к сетям, предназначенным для передачи как данных, так и голоса, и использует цифровые каналы связи в режиме коммутации каналов магистральных, региональных, территориальных и корпоративных сетей. Технология *ISDN* разрабатывалась как основа всемирной телекоммуникационной сети, позволяющей связывать как телефонных абонентов, так и абонентов других глобальных сетей – компьютерных, телексных.

Сети имели большее распространение, так как:

• цифровую технологию можно использовать для передачи любой информации по одному каналу (акустических сигналов, телевизионных видеоданных, факсимильных данных);

• у цифровых методов меньше ограничений передачи и хранения, чем у аналоговых.

В сетях *ISDN* при передаче аналогового сигнала осуществляется преобразование его в последовательность цифровых значений, а при приеме – обратное преобразование. Цифровые сигналы принимаются надежнее, их можно полностью восстановить, прежде чем они из-за затухания станут ниже порогового значения.

Адресация в сети строится по телефонному принципу. Номер *ISDN* состоит из 15 десятичных цифр и включает в себя код страны, код сети и код местной подсети. Код страны такой же, как в обычной телефонной сети. По коду сети выполняется переход в заданную сеть *ISDN*. Внутри подсети для адресации используются 35 десятичных цифр, что позволяет детально идентифицировать любое устройство.

Основное достоинство сетей *ISDN* – то, что они позволяют объединить в единое целое различные виды связи (видео-, аудиопередачу данных). Можно, например, одновременно осуществлять связь нескольких видов: беседовать по видеотелефону и по ходу разговора выводить на экран компьютеров схемы, графики, тексты и т. д.

Скорости передачи данных, реализуемые сетью: 64 кб/с, 128 кб/с, в более дорогих системах – до 2 Мб/с, а в мощных сетях на широкополосных каналах связи – до 155 Мб/с.

Пользовательские интерфейсы сетей ISDN

Внутрисетевой интерфейс базируется на цифровых каналах трех типов:

• *B* – основной канал передачи пользовательских данных со скоростью передачи данных 64 кб/с;

• *D* – канал передачи управляющей (адресной) информации, на основании которой выполняется коммутация каналов (может передавать и пользовательские данные с низкой скоростью) со скоростью передачи 16 или 64 кб/с;

• *H* – канал высокоскоростной передачи пользовательских данных со скоростями передачи 384 (канал *H*0), 1536 (канал *H*11), 1920 (канал *H*12) кб/с.

На основании этих каналов сеть *ISDN* поддерживает два типа пользовательских интерфейсов:

1. Начальный пользовательский интерфейс *BRI* (*Basic Rate Interface*) выделяет пользователю два канала *B* для передачи данных, один канал *D* (16 кб/с) для передачи управляющей информации (формат 2*B*+*D*) и обеспечивает общую пропускную способность 192 кб/с.

2. Основной пользовательский интерфейс – интерфейс первичной скорости *PRI* (*Primary Rate Interface*) обеспечивает пользователей более скоростной передачей данных. Суммарная пропускная способность составляет 2048 кб/с в Европе и 1544 кб/с на других континентах.

Интеграция разнородных трафиков в сети *ISDN* выполняется по принципу временного разделения *time division multiplexing* (*TDM*).

Преобразование аналоговых сигналов в цифровые происходит различными методами. Один из них – импульсно-кодовая модуляция (ИКМ), при использовании которой процесс преобразования включает три этапа: отображение, квантование и кодирование (рис. 11.1).

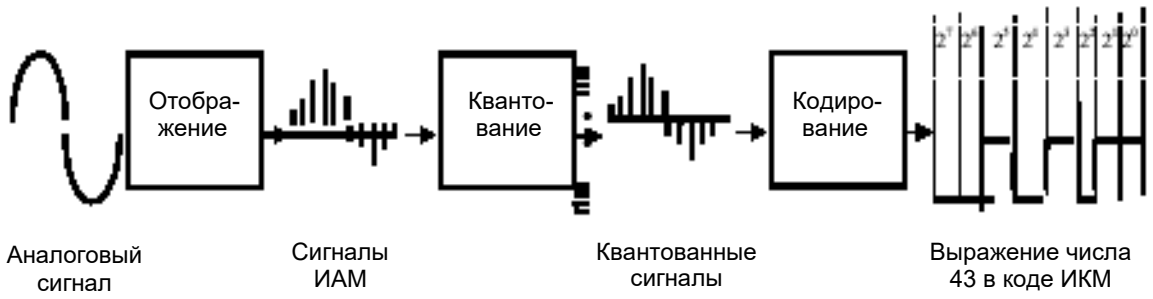


Рис. 11.1. Этапы преобразования аналоговых сигналов в цифровые

Отображения акустических сигналов, каждое из которых называется сигналом импульсно-амплитудной модуляции (ИАМ), запоминаются, а затем трансформируются в двоичные образы.

На этапе квантования каждому сигналу ИАМ придается квантованное значение, соответствующее ближайшему уровню квантования. Весь диапазон изменения амплитуды сигналов ИАМ разбивается на 128 или 256 уровней квантования. Чем больше уровней квантования, тем точнее амплитуда сигнала ИАМ представляется квантованным уровнем.

На этапе кодирования каждому квантованному отображению ставится в соответствие 8-разрядный (при 256-шаговом квантовании) дво-

ичный код. На рисунке показаны сигналы 8-элементного двоичного кода 00101011, соответствующего квантовому сигналу с уровнем 43.

В современных *ISDN* используется и другая концепция преобразования аналоговых сигналов в цифровые, при которой квантуются и затем кодируются не сами сигналы ИАМ, а лишь их изменения, причем число уровней квантования принимается таким же. Очевидно, что такая концепция позволяет производить преобразование сигналов с большей точностью.

Для иллюстрации взаимодействия различных частей *ISDN* рассмотрим рис. 11.2.

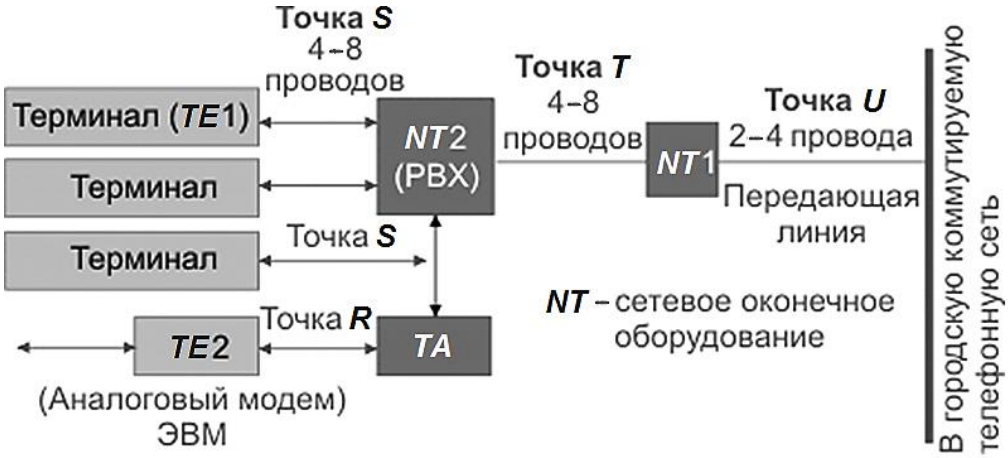


Рис. 11.2. Традиционная схема сети *ISDN*

Сетевой терминал (*NT*-1) представляет собой прибор, который преобразует 2-проводную *ISDN*-линию (от телефонной компании), называемую *u*-интерфейсом, в 8-проводный *S/T*-интерфейс. Как правило, к точке *T* может быть подключено только одно оконечное устройство. *NT*2 же предназначено для подключения большого числа разнотипного оборудования (функции *NT*1 и *NT*2 могут быть совмещены в одном приборе).

Интерфейс *NT*2 может обеспечивать внутриофисный трафик, образуя шину, к которой может подключаться несколько терминалов. Терминальное оборудование (*TE*) в режиме точка-точка может быть подключено к системе кабелем длиной до 1 км, реальным ограничением служит ослабление в 6 дБ на частоте 96 кГц.

В режиме точка-мультиточка (до 8 терминалов) подсоединение производится параллельно, но длина шины в этом случае не должна

превышать 200 м (по временным ограничениям). Оборудование, следующее рекомендациям *ISDN*, может подключаться в точках *S* и *T*.

Стек протоколов сетей ISDN

В сетях *ISDN* определены протоколы только трех нижних уровней.

На физическом уровне используется протокол по стандарту 1/430/431 (при подключении сетевого терминала к коммутатору *ISDN* используются кадры длиной 240 бит).

На канальном уровне управление процессами передачи данных осуществляется путем формирования вызовов. Для передачи управляющей информации на канальном уровне используется протокол *LAP-D* (*Link Access Procedure D-channel*) – один из протоколов множества *HDLC (High-lever Data Link Control Procedure*), включающего в свой состав также протоколы *LAP-B*, используемые в сетях *X*.25, и *LAP-M*, работающие в современных модемах. Протоколы множества *HDLC* передают данные в виде кадров переменной длины.

На сетевом уровне используется либо протокол *X*.25 (коммутаторы сетей *ISDN* выполняют роль коммутаторов *X*.25), либо протокол *Q*.931, выполняющий маршрутизацию с коммутацией каналов.

Основные достоинства сетей *ISDN*:

- предоставление пользователю широкого круга качественных услуг: передача данных, телефония, объединение ЛВС, доступ к *Internet*, передача видео- и аудиотрафика;
- использование обычных двухпроводных линий связи с мультиплексированием одного канала между несколькими абонентами;
- более высокая, нежели при работе с традиционными модемами, скорость передачи информации по телефонным каналам связи – до 128 кб/с на один канал.

Недостатки сетей:

- большие единовременные затраты при создании и модернизации сети;
- синхронное использование каналов связи, не позволяющее динамически подключать к работающему каналу новых абонентов;
- отсутствие скоростной службы коммутации пакетов и невысокие скорости каналов.

Модификации технологии цифровых каналов связи ISDN

Из активно развивающихся цифровых систем следует отметить технологию цифровых абонентских линий *DSL* (*Digital Subscriber Line*), которая обеспечивает высокоскоростную передачу данных на участке витой пары, соединяющей абонента с ближайшей АТС.

Технология *HDSL* является высокоскоростным воплощением *ISDN* и использует четырехуровневую амплитудно-импульсную модуляцию, при которой одним импульсом можно передавать два бита информации. Передача ведется в дуплексном режиме со скоростью до 2,048 Мб/с при использовании двух или трех пар проводов.

Разновидности *HDSL*:

- *SDSL* (*Symmetric DSL*) – использует только одну пару проводов;
- *RADSL* (*Raite Adaptive DSL*) – обеспечивает возможность выбора линейной скорости передачи;
- *MSDSL* (*Multirate SDSL*) – обеспечивает возможность динамически изменять информационную скорость;
- *ADSL* (*Asymmetric DSL*) – для доступа к информационным ресурсам *Internet*.

Асимметричность состоит в увеличении скорости передачи в одном направлении за счет снижения этой скорости в другом. При получении абонентом информации из сети *Internet* скорость может достигать 8 Мб/с, тогда как в обратном направлении – 1,5 Мб/с.

11.3. Сети и технологии *PDH*

Плезиохронная цифровая иерархия (*Plesiochronous Digital Hierarchy, PDH*) – это принцип построения цифровых систем передачи, которые используют групповой мультиплексированный сигнал, состоящий из цифровых 30-канальных потоков (2,048 Мб/с) и требующий синхронизации скоростей цифровых потоков на входе оборудования группообразования.

Под термином «плезиохронные» (то есть «почти синхронные») понимается то, что скорости входных 30-канальных групп немного отличаются друг от друга вследствие допустимой нестабильности задающего генератора каналообразующего оборудования этих потоков. Поэтому прежде чем приступить к объединению этих потоков в 2,048 Мб/с, их нужно привести к одной скорости передачи путем добавления специальных синхронизирующих битов выравнивания скоростей.

Биты выравнивания должны распознаваться на приемной стороне, когда происходит разделение (демультиплексирование) потоков из группового и выделение первоначального сигнала. Такой групповой сигнал, состоящий из нескольких элементарных плезиохронных 30-канальных групп, и называется *PDH*.

Начало *технологии PDH* было положено разработкой мультиплексора *T*-1, который позволял в цифровом виде мультиплексировать, передавать и коммутировать (на постоянной основе) голосовой трафик 24 абонентов. Так как абоненты по-прежнему пользовались обычными телефонными аппаратами, то есть передача голоса шла в аналоговой форме, то *T*-1 сами оцифровывали голос с частотой 8000 Гц и кодировали его методом импульсно-кодовой модуляции. В результате каждый абонентский канал образовывал цифровой поток данных 64 кб/с, а мультиплексор *T*-1 обеспечивал передачу 1,544 Мб/с.

Для соединения крупных телефонных станций каналы *T*-1 представляли собой слабые и негибкие средства мультиплексирования, поэтому была реализована идея образования каналов с *иерархией скоростей.*

Четыре канала типа *T*-1 объединили в канал следующего уровня цифровой иерархии – *T*-2, передающий данные со скоростью 6,312 Мб/с.

Канал *T*-3, образованный путем объединения 7 каналов *T*-2, имеет скорость 44,736 Мб/с.

Канал *T*-4 объединяет 6 каналов *T*-3, в результате его скорость равна 274 Мб/с. Эта технология получила название системы *T*-каналов.

С середины 1970-х гг. выделенные каналы, построенные на основе систем *T*-каналов, стали сдаваться телефонными компаниями в аренду на коммерческих условиях. Они позволяют передавать не только голос, но и любые данные, представленные в цифровой форме, – компьютерные данные, телевизионное изображение, факсы и т. п.

Технология систем *T*-каналов была стандартизована Американским национальным институтом стандартов (*ANSI*), а позже – Международным комитетом *CCITT*. При стандартизации она получила название *PDH*. В результате внесенных комитетом *CCITT* изменений возникла несовместимость американской и международной версий стандарта *PDH*. Аналогом систем *T*-каналов в международном стандарте являются каналы *E*-1, *E*-2 и *E*-3 со скоростями – 2,048, 8,488 и 34,368 Мб/с.

Несмотря на различия в американской и международной версиях технологии цифровой иерархии, принято использовать одни и те же обозначения для иерархии скоростей – *DSn* (*Digital Signal n*). Далее в таблице приводятся значения для всех введенных стандартами уровней скоростей обеих технологий.

Иерархия цифровых скоростей

Обозначение скорости	*ANSI* (Америка)			*CCITT* (Европа)		
	Кол-во голосовых каналов	Количество каналов предыдущего уровня	Скорость, Мб/с	Кол-во голосовых каналов	Количество каналов предыдущего уровня	Скорость, Мб/с
DS-0	1	1	0,064	1	1	0,064
DS-1	24 *T*-1	24	1,544	30 *E*-1	30	2,048
DS-2	96 *T*-2	4	6,312	120 *E*-2	4	8,488
DS-3	672 *T*-3	7	44,736	480 *E*-3	4	34,368
DS-4	4032 *T*-4	6	274,176	1920 *E*-4	4	139,264

11.4. Сети и технологии *SDH*

В сетях стандарта *SDH* (*Synchronous Digital Hierarchy* – синхронная цифровая иерархия) реализуется технология синхронных волоконно-оптических сетей. Это высокоскоростные сети цифровой связи, которые строятся на базе оптоволоконных кабельных линий или цифровых радиорелейных линий. Основу инфраструктуры современных высокоскоростных телекоммуникационных сетей (магистральных, региональных или городских) составляют цифровые линии и узлы сети стандарта *SDH*.

При построении сетей *SDH* используются следующие модули:

• *мультиплексоры SDH* – это основные функциональные модули сетей *SDH*, предназначенные для сборки высокоскоростного потока информации из низкоскоростных потоков и разборки высокоскоростного потока на низкоскоростные;

• *коммутаторы* обеспечивают связь каналов, закрепленных за пользователями, путем полупостоянного перекрестного соединения между ними;

• *концентраторы* служат для объединения однотипных потоков нескольких удаленных узлов сети в одном распределенном узле;

• *регенераторы* – это устройства мультиплексирования с одним оптическим каналом доступа и одним-двумя выходами, используемыми для увеличения расстояния между узлами сети *SDH*.

Сети и технологии *SDH* отличаются высоким уровнем стандартизации (что позволяет в одной сети использовать оборудование разных фирм-производителей), высокой надежностью (централизованное управление сетью обеспечивает полный мониторинг состояния узлов), наличием полного программного контроля. Благодаря этим преимуществам технология *SDH* стала основной при построении цифровых транспортных сетей самого различного масштаба.

Топология всей сети *SDH* формируется из отдельных базовых топологий типа «кольцо», «линейная цепь», «звезда», «точка-точка», которые используются в качестве сегментов сети.

Сегмент сети, связывающий два узла A и B, или топология «точка-точка», является наиболее простым примером базовой топологии сети *SDH* (рис. 11.3). Она может быть реализована с помощью терминальных мультиплексоров *TM*, как по схеме без резервирования канала приёма/передачи, так и по схеме со стопроцентным резервированием типа 1+1, использующей основной и резервный электрические или оптические агрегатные выходы (каналы приёма/передачи).

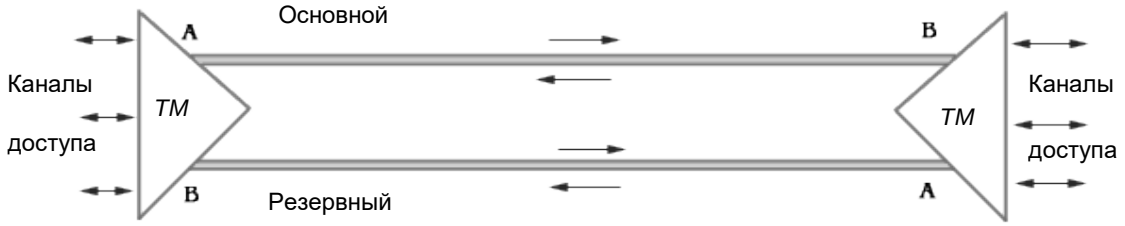


Рис. 11.3. Топология «точка-точка», реализованная с использованием *TM*

Топология *«последовательная линейная цепь»* используется тогда, когда интенсивность трафика в сети не так велика и существует необходимость ответвлений в ряде точек линии, где могут вводиться каналы доступа. Она может быть представлена либо в виде простой последовательной линейной цепи без резервирования, как на рис. 11.4, либо более сложной цепью с резервированием типа 1+1. Здесь *TDM* – тер-

минальный мультиплексор с временным разделением. Последний вариант топологии часто называют упрощённым кольцом.

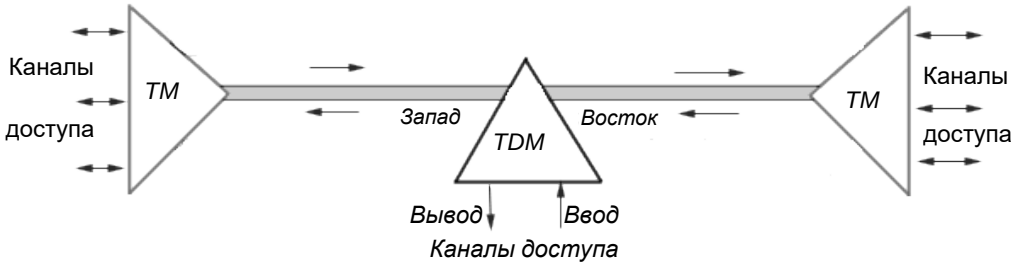


Рис. 11.4. Топология «последовательная линейная цепь», реализованная на *TM* и *TDM*

В топологии *«звезда»*, реализующей функцию концентратора, один из удалённых узлов сети, связанный с центром коммутации или узлом сети *SDH* на центральном кольце, играет роль концентратора, или хаба, где часть трафика может быть выведена на терминалы пользователя, тогда как оставшаяся его часть может быть распределена по другим удалённым узлам (рис. 11.5).

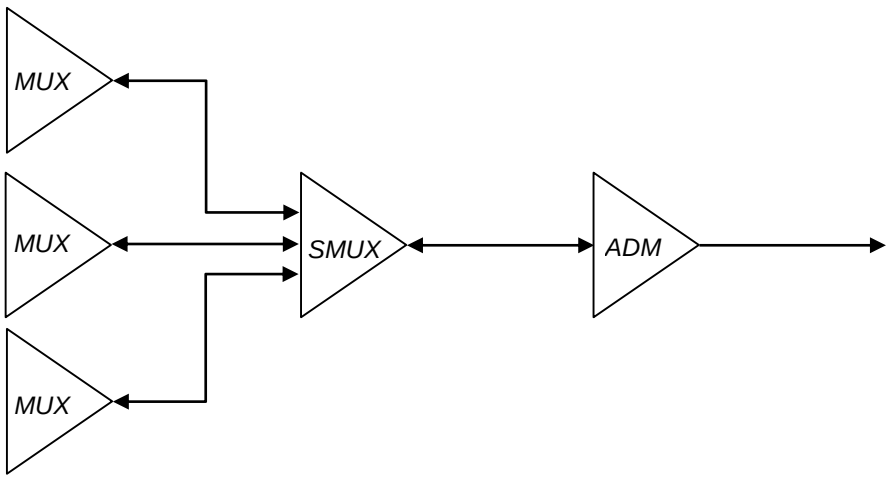


Рис. 11.5. Топология «звезда» с мультиплексором в качестве концентратора

Топология *«кольцо»* (рис. 11.6) широко используется для построения сетей *SDH* первых двух уровней иерархии *SDH* (155 и 622 Мб/с). Основное преимущество этой топологии – лёгкость организации защиты типа 1+1 благодаря наличию в синхронных мультиплексорах

SMUX двух пар оптических каналов приёма/передачи: восток – запад, дающих возможность формирования двойного кольца со встречными потоками.

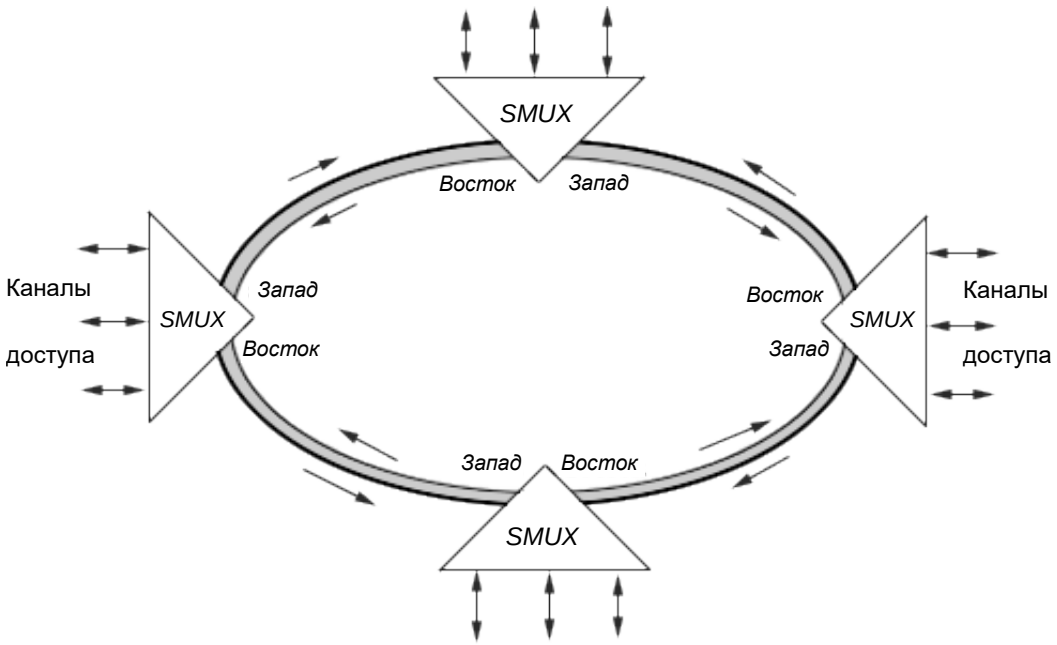


Рис. 11.6. Топология «кольцо» с защитой 1+1

Архитектурные решения при проектировании сети *SDH* могут быть сформированы на базе использования рассмотренных выше элементарных топологий сети в качестве её отдельных сегментов.

Пример радиально-кольцевой архитектуры сети *SDH* приведён на рис. 11.7. Эта сеть фактически построена на базе использования двух базовых топологий: «кольцо» и «последовательная линейная цепь».

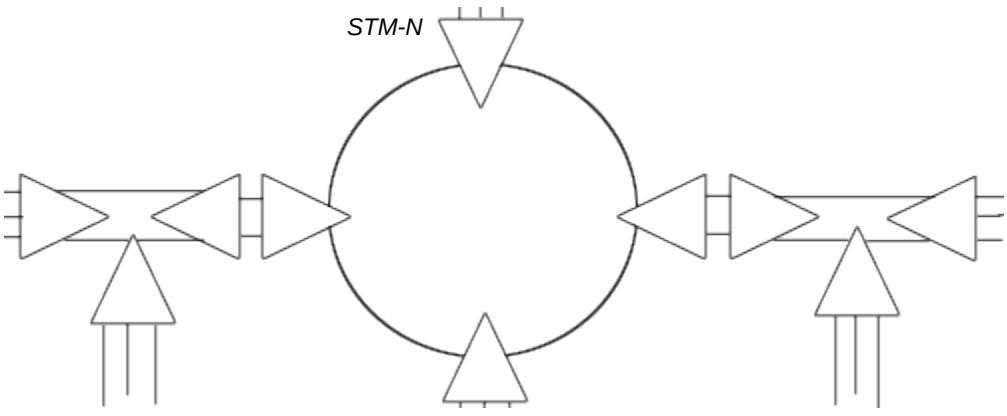


Рис. 11.7. Радиально-кольцевая сеть *SDH*

Преимущества сетей *SDH/SONET*

1. Гибкая иерархическая схема мультиплексирования цифровых потоков разных скоростей, позволяющая вводить в магистральный канал и выводить из него пользовательскую информацию любого поддерживаемого уровня скорости, не демультиплексируя поток.

2. Отказоустойчивость сети. Сети *SDH* обладают высокой степенью «живучести» – технология предусматривает автоматическую реакцию оборудования на такие типичные отказы, как обрыв кабеля, отказ порта, выход из строя мультиплексора или отдельной его карты, направляя трафик по резервному пути или переходя на резервный модуль. Переход на резервный путь происходит очень быстро – обычно в течение 50 мс.

3. Мониторинг и управление сетью осуществляется на основе информации, встроенной в заголовки кадров. Это обеспечивает обязательный уровень управляемости сети, не зависящий от производителя оборудования, и создает основу для наращивания функций менеджмента в фирменных системах управления.

4. Высокое качество транспортного обслуживания для трафика любого типа (голос, видео и данные). В основе *SDH* – техника временного мультиплексирования *TDM*, обеспечивающая каждому абоненту гарантированную пропускную способность, а также низкий и фиксированный уровень задержек.

Недостатки – неспособность динамически перераспределять пропускную способность между абонентами сети, т.е. то, что обеспечивается пакетными сетями.

В России наибольшую активность в использовании *SDH*-технологии проявляет АО «Ростелеком», которое ежегодно строит 5 – 6 тыс. км магистральных цифровых линий на основе волоконно-оптических кабелей (ВОЛС) и цифровых радиорелейных линий. Компанией *RASCOM* построена в 1994 г. и эксплуатируется высокоскоростная цифровая оптоволоконная магистральная линия стандарта *SDH* между Москвой и Санкт-Петербургом протяженностью 690 км.

Технология *SDH* может легко интегрироваться с технологией *DWDM* (*Dense Wave Division Multiplexing* – плотное волновое (спектральное) мультиплексирование), обеспечивающей передачу информации по оптическим магистралям с еще более высокими скоростями (сотни гигабит в секунду и выше) за счет мультиплексирования с разделением по длине волны.

В магистральных сетях с ядром *DWDM* сети *SDH* будут играть роль сети доступа, то есть ту же роль, которую играют сети *PDH* по отношению к *SDH*.

11.5. Сети и технологии *DWDM*

Технология *DWDM* предназначена для создания оптических магистралей нового поколения, работающих на мультимегабитных и терабитных скоростях.

Такой качественный скачок происходит из-за принципиально иного, чем в *SDH*, метода мультиплексирования – информация в оптическом волокне передается одновременно большим количеством световых волн. Сети *DWDM* работают по принципу *коммутации каналов*, при этом каждая световая волна представляет собой отдельный *спектральный канал* и несет собственную информацию.

При этом устройства *DWDM* занимаются только объединением различных волн в одном световом пучке, а также выделением из общего сигнала информации каждого спектрального канала.

На рис. 11.8, *а* показана типовая схема *DWDM*-мультиплексора с зеркальным отражательным элементом. Рассмотрим его работу в режиме демультиплексирования. Приходящий мультиплексный сигнал попадает на входной порт. Затем этот сигнал проходит через волноводпластину и распределяется по множеству волноводов, представляющих дифракционную структуру *AWG* (*arrayed waveguide grating*).

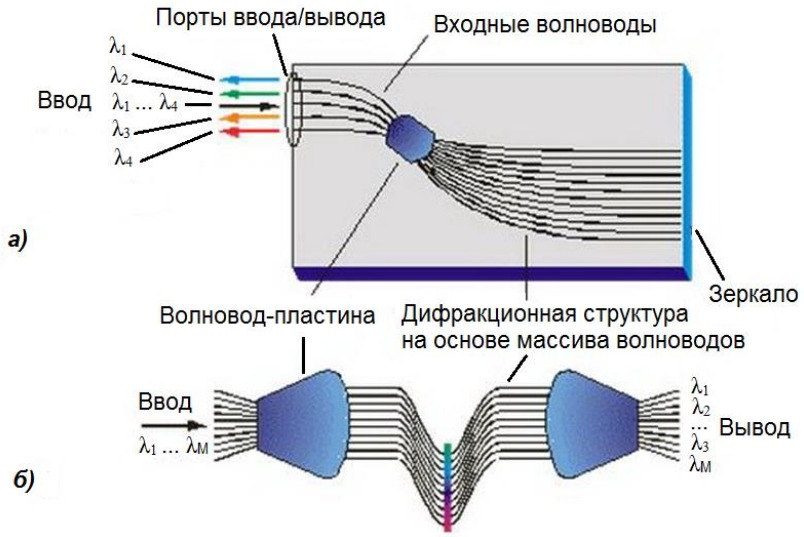


Рис. 11.8. *DWDM*-мультиплексор

По-прежнему сигнал в каждом из волноводов остается мультиплексным, а каждый канал остается представленным во всех волноводах. Далее происходит отражение сигналов от зеркальной поверхности и в итоге световые потоки вновь собираются в волноводе-пластине, где происходит их фокусировка и интерференция – образуются пространственно-разнесенные интерференционные максимумы интенсивности, соответствующие разным каналам. Геометрия волновода-пластины, в частности расположение выходных полюсов, и длины волноводов структуры *AWG* рассчитываются таким образом, чтобы интерференционные максимумы совпадали с выходными полюсами. Мультиплексирование происходит обратным путем (рис. 11.8, *б*).

Городские сети *DWDM*, как правило, строят с использованием кольцевой архитектуры, что позволяет применять механизмы защиты на уровне *DWDM* при скорости восстановления не более 50 мс. Возможно построение сетевой инфраструктуры на оборудовании нескольких поставщиков с дополнительным уровнем распределения на базе оборудования *Metro DWDM*. Этот уровень вводится для организации обмена трафиком между сетями с оборудованием разных фирм.

Пример построения городской сети *DWDM* приведен на рис. 11.9.

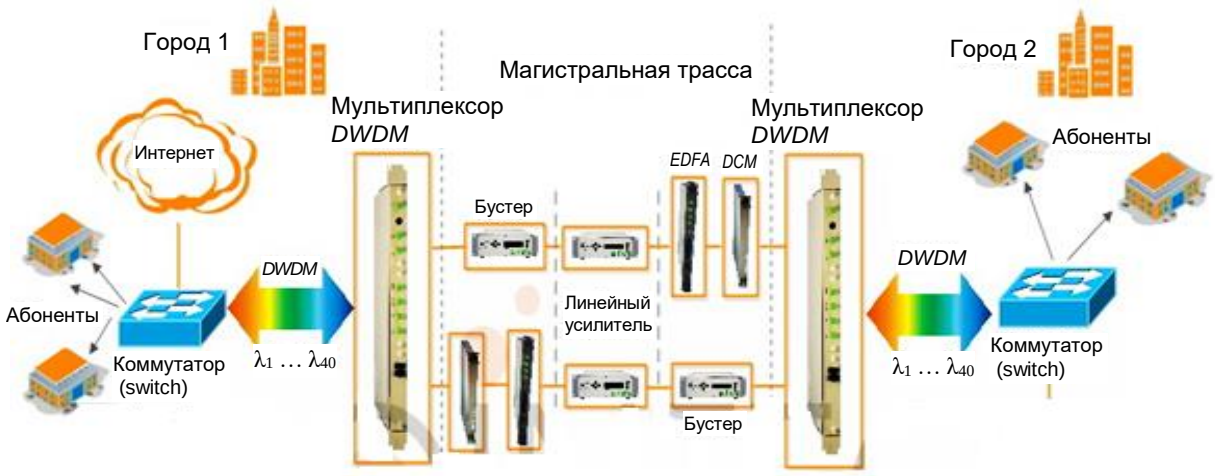


Рис. 11.9. Построение городской сети *DWDM*

При использовании оборудования разных производителей две подсети передачи данных одного производителя соединяют через сеть *DWDM* другого производителя. Здесь бустеры обеспечивают усиление

оптического сигнала *CDMA* сразу для нескольких устройств. *DCM* – высокоскоростной кабельный модем. Усилитель оптического сигнала *EDFA* (*Erbium Doped Fibre Amplifier*) на основе примесного оптического волокна, легированного эрбием, предназначен для усиления оптического сигнала в сетях *DWDM*. Система управления, подсоединенная физически к одной подсети, может управлять и работой другой подсети. Если бы на уровне распределения использовалось *SDH*-оборудование, то это было бы невозможно. Таким образом, на базе сетей *DWDM* можно объединять сети разных производителей для передачи разнородного трафика.

11.6. Сеть и технология *X*.25

Сеть *X*.25 – *классическая полнопротокольная сеть,* разработанная Международной организацией по стандартизации (*ISO*). Эта сеть явилась базой информационного обмена региональных и общероссийских органов управления, иных корпоративных структур.

Главная особенность сети *X*.25 – *использование виртуальных каналов* для обеспечения информационного взаимодействия между компонентами сети. Виртуальные каналы предназначены для организации вызова и непосредственной передачи данных между абонентами сети. Информационный обмен в сети *X*.25 во многом похож на аналогичный процесс в сетях *ISDN* и состоит из трех обязательных фаз:

1) установление вызова (виртуального канала);

2) информационный обмен по виртуальному каналу;

3) разрывание вызова (виртуального канала).

На рис. 11.10 представлена структурная схема сети *X*.25, где изображены основные элементы:

- *DTE* (*data terminal equipment*) – аппаратура передачи данных (кассовые аппараты, банкоматы, терминалы бронирования билетов, ПК и другое оконечное оборудование пользователей).
- *DCE* (*data circuit-terminating equipment*) – оконечное оборудование канала передачи данных (телекоммуникационное оборудование, обеспечивающее доступ к сети).
- *PSE* (*packet switching exchange*) – коммутаторы пакетов.

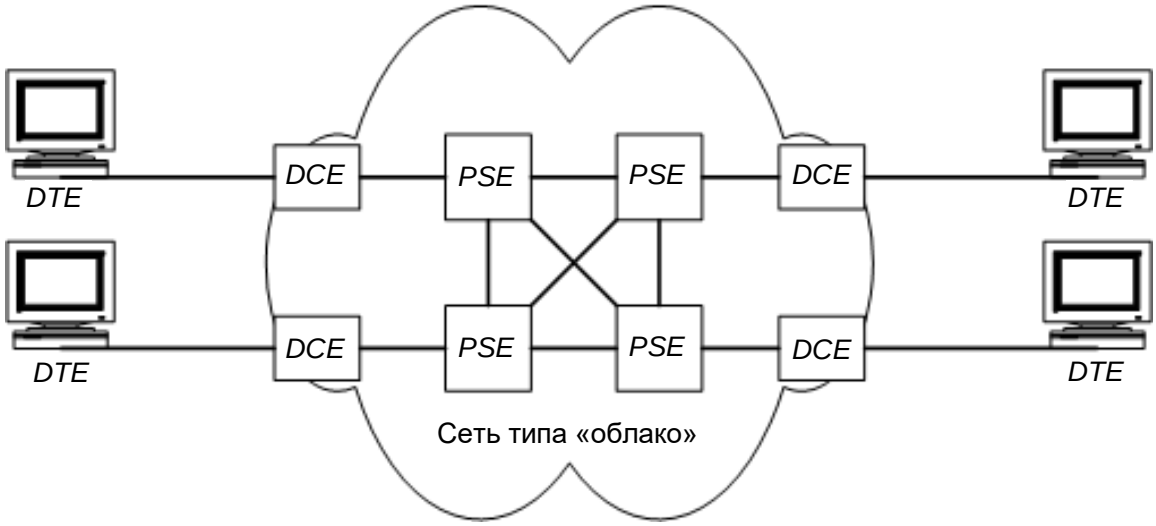


Рис. 11.10. Структурная схема сети *X*.25

Интерфейс *X*.25 обеспечивает:

1) доступ удаленному пользователю к главному компьютеру;

2) доступ удаленному ПК к локальной сети;

3) связь удаленной сети с другой удаленной сетью.

Интерфейс *X*.25 содержит три нижних уровня модели *OSI*: физический, канальный и сетевой. Особенность сети – использование коммутируемых виртуальных каналов для осуществления передачи данных между компонентами сети. Установление коммутируемого виртуального канала выполняется служебными протоколами, выполняющими роль протокола сигнализации.

На физическом уровне X.25 используются аналоговые выделенные линии, которые обеспечивают двухточечное соединение. Могут использоваться аналоговые телефонные линии, а также цифровые выделенные линии. На сетевом уровне нет контроля достоверности и управления потоком. На физическом уровне *X*.25 реализуется один из протоколов *X*.21 или *X*.21*bis*.

На канальном уровне сеть X.25 обеспечивает гарантированную доставку, целостность данных и контроль потока. На канальном уровне поток данных структурируется на кадры. Контроль ошибок производится во всех узлах сети. При обнаружении ошибки выполняется повторная передача данных. Канальный уровень реализуется протоколом *LAP-B*, который работает только с двухточечными каналами связи, поэтому адресация не требуется.

Сетевой уровень X.25 реализуется протоколом *PLP* (*Packet-Layer Protocol* – протокол уровня пакета). На сетевом уровне кадры объединяются в один поток, а общий поток разбивается на пакеты. Протокол *PLP* управляет обменом пакетов через виртуальные цепи. Сеанс связи устанавливается между двумя устройствами *DTE* по запросу от одного из них. Максимальная длина поля адреса устройства *DTE* в пакете *X.*25 составляет 16 байт. После установления коммутируемой виртуальной цепи эти устройства могут вести полнодуплексный обмен информации. Сеанс может быть завершен по инициативе любого *DTE*, после чего для последующего обмена снова потребуется установление соединения.

Пакет протокола *X.*25 состоит как минимум из трех байтов, которые определяют заголовок пакета. Первый байт содержит четыре бита идентификатора общего формата и четыре бита номера группы логического канала. Второй байт содержит номер логического канала, а третий – идентификатор типа пакета. Пакеты в сети бывают двух типов:

1. управляющие пакеты;
2. пакеты данных.

Тип пакета определяется значением младшего бита идентификатора типа пакета.

Сетевые адреса получателя и отправителя пакета состоят из двух частей:

1. *Data Network ID Code* (*DNIC*) – содержит 4 десятичные цифры, определяющие код страны и номер провайдера;
2. *Network Terminal Number* – содержит 10 или 11 десятичных цифр, которые провайдер определяет для идентификации конкретного пользователя.

Сборку, а затем разборку пакетов выполняет специальное устройство «сборщик-разборщик пакетов» (*PAD, Packet Assembler Disassembler*).

Достоинства сети *X.*25:

- гарантированная доставка пакетов;
- высокая надежность сети ввиду постоянного эффективного контроля за появлением ошибок и наличия механизма альтернативной маршрутизации;
- возможность работы в любых каналах.

Недостатки сети *X.*25:

- невысокая скорость передачи данных – обычно в пределах от 56 до 64 кб/с;

• невозможность передавать чувствительный к временным задержкам трафик (оцифрованный голос, видеоинформацию).

11.7. Сеть и технология *Frame Relay*

Сеть *Frame Relay* является сетью с коммутацией кадров или сетью с ретрансляцией кадров, ориентированной на использование цифровых линий связи. Первоначально технология *Frame Relay* (*FR*) была стандартизирована как служба в сетях *ISDN* со скоростью передачи данных до 2 Мб/с.

В дальнейшем эта технология получила самостоятельное развитие. *Frame Relay* поддерживает физический и канальный уровни *OSI*, Технология *Frame Relay* для передачи данных использует технику виртуальных соединений (коммутируемых и постоянных).

Стек протоколов *Frame Relay* передает кадры при установленном виртуальном соединении по протоколам физического и канального уровней. В *Frame Relay* функции сетевого уровня перемещены на канальный уровень, поэтому необходимость в сетевом уровне отпала. На канальном уровне в *Frame Relay* выполняется мультиплексирование потока данных в кадры.

Каждый кадр канального уровня содержит заголовок, содержащий номер логического соединения, который используется для маршрутизации и коммутации трафика. *Frame Relay* осуществляет мультиплексирование в одном канале связи нескольких потоков данных. Кадры при передаче через коммутатор не подвергаются преобразованиям, поэтому сеть получила название ретрансляции кадров. Таким образом, сеть коммутирует кадры, а не пакеты. Скорость передачи данных до 44 Мб/с, но без гарантии целостности данных и достоверности их доставки.

Frame Relay ориентирована на цифровые каналы передачи данных хорошего качества, поэтому в ней отсутствует проверка выполнения соединения между узлами и контроль достоверности данных на канальном уровне. Кадры передаются без преобразования и контроля как в коммутаторах локальных сетей. За счет этого сети *Frame Relay* обладают высокой производительностью. При обнаружениях ошибок в кадрах повторная их передача не выполняется, а искаженные – отбраковываются. Достоверность данных контролируется на более высоких уровнях модели *OSI*.

Сети *Frame Relay* широко используются в корпоративных и территориальных сетях в качестве:

- каналов для обмена данными между удаленными локальными сетями (в корпоративных сетях);
- каналов для обмена данными между локальными и территориальными (глобальными) сетями.

Технологию *Frame Relay* в основном применяют для маршрутизации протоколов локальных сетей через общие (публичные) коммуникационные сети. *Frame Relay* обеспечивает передачу данных с коммутацией пакетов через интерфейс между оконечными устройствами пользователя *DTE* (маршрутизаторами, мостами, ПК) и оконечным оборудованием канала передачи данных *DCE* (коммутаторами сети типа «облако»).

Коммутаторы *Frame Relay* используют технологию сквозной коммутации, т.е. кадры передаются с коммутатора на коммутатор сразу после прочтения адреса назначения, что обеспечивает высокую скорость передачи данных. В сетях *Frame Relay* применяются высококачественные каналы передачи, поэтому возможна передача трафика, чувствительного к задержкам (голосовых и мультимедийных данных). В магистральных каналах сети *Frame Relay* применяют волоконно-оптические кабели, а в каналах доступа может применяться высококачественная витая пара.

На рис. 11.11 представлена структурная схема сети *Frame Relay*, где изображены основные элементы:

- *DTE* (*data terminal equipment*) – аппаратура передачи данных (маршрутизаторы, мосты, ПК).
- *DCE* (*data circuit-terminating equipment*) – оконечное оборудование канала передачи данных (телекоммуникационное оборудование, обеспечивающее доступ к сети).

Рис. 11.11. Структурная схема сети *Frame Relay*

На физическом уровне Frame Relay используют цифровые выделенные каналы связи, реализуемые протоколом физического уровня *I*.430/431.

На канальном уровне поток данных структурируется на кадры, поле данных в кадре имеет переменную величину, но не более 4096 байт. Канальный уровень реализуется протоколом *LAP-F*.

В поле заголовка кадра имеется информация, которая используется для управления виртуальным соединением в процессе передачи данных. Виртуальному соединению присваивается определенный номер (*DLCI*). *DLCI* (*Data Link Connection Identifier*) – идентификатор соединения канала данных. Каждый кадр канального уровня содержит номер логического соединения, который используется для маршрутизации и коммутации трафика. При этом правильную передачу данных от отправителя к получателю контролирует на более высоком уровне модели *OSI*.

В сети *Frame Relay* используются два типа виртуальных каналов: постоянные (*PVC*) и коммутируемые виртуальные каналы. Коммутируемые виртуальные каналы применяются для передачи импульсного трафика между двумя устройствами *DTE*, постоянные – для постоянного обмена сообщениями между двумя устройствами *DTE*.

Процесс передачи данных через коммутируемые виртуальные каналы происходит следующим образом:

- установление вызова – образуется коммутируемый логический канал между двумя *DTE*;
- передача данных по установленному логическому каналу;
- режим ожидания, когда коммутируемая виртуальная цепь установлена, но обмен данными не происходит;
- завершение вызова – используется для завершения сеанса; конкретное виртуальное соединение разрывается.

Данные через предварительно установленные постоянные виртуальные каналы передаются следующим образом:

- передача данных по установленному логическому каналу;
- режим ожидания, когда коммутируемая виртуальная цепь установлена, но обмен данными не происходит.

Достоинства сети Frame Relay:

- высокая надежность работы сети;

• обеспечивает передачу чувствительного к временным задержкам трафика (голос, видеоизображение).

Недостатки сети Frame Relay:

• высокая стоимость качественных каналов связи;

• не обеспечивается достоверность доставки кадров.

11.8. Сеть и технология *ATM*

Технология *ATM* (*Asynchronous Transfer Mode – режим асинхронной передачи*) – это одна из самых перспективных технологий построения высокоскоростных сетей любого класса – от локальных до глобальных. Термин «асинхронный» в названии технологии указывает на ее отличие от синхронных технологий с фиксированным распределением пропускной способности канала между информационными потоками (например, *ISDN*).

В основе транспортного механизма *ATM* лежит технология широкополосной *ISDN* (*B-ISDN, Broadband ISDN*), призванная обеспечить возможность создания единой, универсальной, высокоскоростной сети взамен множества сложных неоднородных существующих сетей. Основные компоненты сети *ATM*:

ATM-коммутаторы (*ATM Switch*), представляющие собой быстродействующие специализированные вычислительные устройства;

Адаптеры – *Customer Premises Equipment* (*CPE*), обеспечивающие адаптацию информационных потоков пользователя при передаче с использованием технологии *ATM*.

Коммутатор *ATM* состоит:

• из коммутатора виртуальных путей;

• коммутатора виртуальных каналов.

Эта особенность организации *ATM* обеспечивает дополнительное увеличение скорости обработки ячеек.

Передача информации в сетях *ATM* происходит после предварительного установления соединений, выполняемого высокоскоростными коммутаторами *ATM*. Коммутаторы создают широкополосный физический канал, в котором динамически можно формировать более узкополосные виртуальные подканалы. Передаются по каналу не кадры, не пакеты, а

ячейки (*cells*). Ячейка представляет собой очень короткие последовательности байтов – размер ячейки 53 байта, включая заголовок (5 байт). Ячейки передаются по сети, не занимая конкретных временных интервалов, как это имеет место в *B*-каналах сетей *ISDM*.

Технология *ATM* совмещает в себе подходы двух технологий – коммутации пакетов и коммутации каналов. От первых заимствована передача адресуемых пакетов, от вторых – минимизация задержек в сети ввиду пакетов малого размера.

Скорость передачи данных по каналам *ATM* лежит в пределах от 155 до 2200 Мб/с. При скорости 155 Мб/с время передачи ячейки длиной 53 байта составит менее 3 мкс.

Технология рассчитана на работу с трафиками разного типа.

В существующих спецификациях технологии определены пять классов трафика:

- класс *A* – синхронный трафик с предварительным установлением соединения и постоянной битовой скоростью (отсутствие пульсаций). Примеры: голосовой трафик и видеотрафик;
- класс *B* – синхронный трафик с предварительным установлением соединения и переменной битовой скоростью (наличие пульсаций). Примеры: компрессированные аудио- и видеотрафики;
- класс *C* – асинхронный трафик с предварительным установлением соединения и переменной битовой скоростью (наличие пульсаций). Примеры: трафик компьютерных сетей с коммутацией пакетов (*X*.25, *Frame Relay*, *TCP/IP* и т.д.);
- класс *D* – асинхронный трафик без предварительного установления соединения и переменной битовой скоростью (наличие пульсаций). Примеры: трафик компьютерных сетей типа *Ethernet* и т.п.;
- класс *X* – тип трафика определяется пользователем.

Режим асинхронной передачи основан на концепции двух оконечных пунктов сети (абонентских систем, терминалов), осуществляющих связь друг с другом через совокупность промежуточных коммутаторов. При этом используются интерфейсы двух типов:

- интерфейс пользователя с сетью (*UNI – User-to-Network Interface*);
- интерфейс между сетями (*NNI – Network-to-Network Interface*).

Структурная схема сети на основе технологии *ATM* показана на рисунке 11.12. *UNI* соединяет устройство оконечного пользователя с общедоступным или частным *ATM*-коммутатором, а *NNI* представляет собой канал связи между двумя *ATM*-коммутаторами сети.

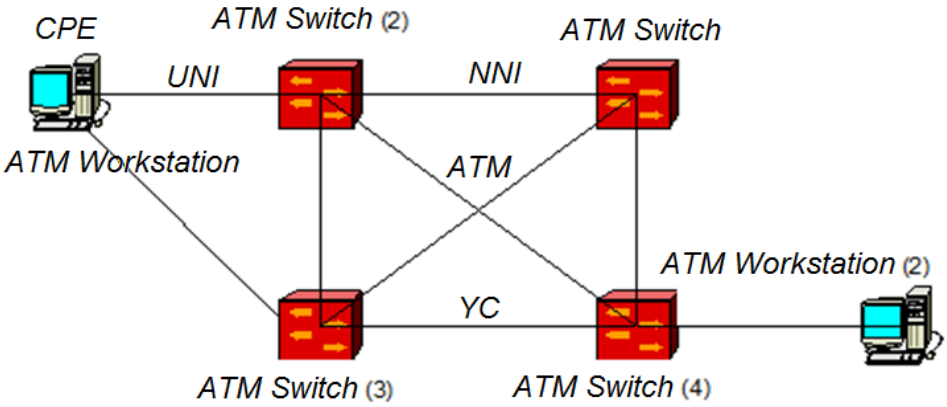


Рис. 11.12. Структурная схема сети на основе технологии *ATM*

Соединение между двумя оконечными пунктами сети (напомним, что *ATM*-технология ориентирована на предварительное установление соединения) возникает с того момента, когда один из них передает через *UNI* запрос в сеть. Этот запрос через цепочку *ATM*-коммутаторов отправляется в пункт назначения для интерпретации.

Если узел-адресат принимает запрос на соединение, то в *ATM*-сети между двумя пунктами организуется виртуальный канал.

UNI-устройства этих пунктов и промежуточные узлы сети (т.е. *ATM*-коммутаторы) обеспечивают правильную маршрутизацию ячеек за счет того, что каждая *ATM*-ячейка содержит два поля – идентификатор виртуального пути (*VPI – Virtual Path Identifier*) и идентификатор виртуального канала (*VCI – Virtual Circuit Identifier*). Виртуальный путь представляет собой группу виртуальных каналов, которые в пределах данного интерфейса имеют одинаковое направление передачи данных.

Информация, содержащаяся в полях *VPI* и *VCI* *ATM*-ячейки, используется для однозначного решения задачи маршрутизации даже в случае, если у оконечной системы организовано несколько виртуальных связей.

Вопросы к компьютерному тестированию

1. Какие сетевые технологии используют обычные двухпроводные линии связи с мультиплексированием одного канала между несколькими абонентами?
2. Какие сетевые технологии используют временное мультиплексирование?
3. Какие сетевые технологии используют уплотненное волновое мультиплексирование?
4. В какой сетевой технологии используют спектральное разделение передаваемого сигнала?
5. Какие сетевые технологии предназначены для передачи как данных, так и голоса?
6. Какие сетевые технологии реализуются в виде технологии синхронных волоконно-оптических сетей?
7. Какие сетевые технологии используют виртуальные каналы для обеспечения информационного взаимодействия между компонентами сети?
8. Какая сетевая технология является сетью с гарантированной доставкой информации?
9. Какая сетевая технология является сетью с гарантированной согласованной скоростью передачи информации?
10. Какая сетевая технология совмещает в себе подходы двух технологий – коммутации пакетов и коммутации каналов?
11. Сколько десятичных цифр включает в себя номер *ISDN*?
12. Какие типы каналов включают пользовательские интерфейсы сетей *ISDN*?
13. Какие типы пользовательских интерфейсов поддерживает сеть *ISDN*?
14. Какие этапы включает преобразование аналоговых сигналов при импульсно-кодовой модуляции в сетях *ISDN*?
15. Протоколы каких уровней модели ВОС определены в сетях *ISDN*?
16. Какая сетевая технология использует четырехуровневую амплитудно-импульсную модуляцию?

17. Какое количество цифровых канальных потоков используется в технологии «Плезиохронная цифровая иерархия»?
18. Под каким названием была стандартизована Американским национальным институтом стандартов технология системы *T*-каналов?
19. С какой скоростью происходит передача данных по каналу уровня цифровой иерархии *T*-2 для соединения крупных телефонных станций по технологии системы *T*-каналов?
20. Какие из модулей сетей *SDN* предназначены для сборки/разборки информационных потоков?
21. Какие из модулей сетей *SDN* служат для объединения однотипных потоков?
22. Какие из модулей сетей *SDN* предназначены для увеличения расстояния между узлами сети?
23. Какая из топологий используется в технологии *SDN*, когда интенсивность трафика в сети невелика и существует необходимость ответвлений в ряде точек линии?
24. Какая из топологий используется для построения сетей *SDH* первых двух уровней иерархии *SDH* (155 и 622 Мб/с)?
25. Как называют прием, используемый в технологии цифровых каналов связи и заключающийся в увеличении скорости передачи в одном направлении за счет снижения этой скорости в другом?
26. Что включают байты пакета протокола *X*.25?
27. Протоколы каких уровней модели ВОС наиболее развиты в сетях *X*.25?
28. Какое устройство используется в технологии *Frame Relay* для обеспечения голосовому трафику наивысшего приоритета?
29. Какой класс трафика использует технология *ATM* при передаче голоса и видео?
30. Какой класс трафика использует технология *ATM* в сетях типа *Ethernet*?

Глава 12

СРЕДСТВА ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Рассматриваемые вопросы:

12.1. Линии связи и каналы передачи данных.
12.2. Техническое обеспечение информационно-вычислительных сетей.
12.2.1. Серверы и рабочие станции.
12.2.2. Концентраторы, приемопередатчики и повторители.
12.2.3. Мосты, маршрутизаторы, коммутаторы и шлюзы.
12.2.4. Модемы и факс-модемы.
12.2.5. Сетевые адаптеры и анализаторы.
12.3. Информационное обеспечение сети.
12.4. Программное обеспечение сети.

Средства функционирования ВС включают ***линии связи*** и ***каналы передачи данных***, а также техническое, информационное и программное обеспечение.

Техническое (аппаратное) обеспечение составляют ЭВМ различных типов, средства связи, оборудование абонентских систем, оборудование узлов связи, аппаратура связи и согласования работы сетей различных уровней.

Информационное обеспечение сети представляет собой единый информационный фонд, содержащий массивы данных общего применения, доступные для всех пользователей сети, и массивы индивидуального пользования.

Программное обеспечение (ПО) компьютерных сетей многообразно как по своему составу, так и по выполняемым функциям.

Выделяются следующие группы ПО сетей:

• общесетевое ПО, образуемое средствами, входящими в состав комплекта программ технического обслуживания сети (КПТО), – это

контролирующие тест-программы для контроля работоспособности элементов и звеньев сети и диагностические тест-программы для локализации неисправностей в сети;

- специальное ПО, представленное прикладными программными средствами, библиотеками стандартных программ;
- базовое программное обеспечение ЭВМ абонентских систем, включающее операционные системы ЭВМ, системы автоматизации программирования, контролирующие и диагностические тест-программы.

Рассмотрение средств обеспечения функционирования КС начнем с технического обеспечения.

12.1. Линии связи и каналы передачи данных

Для построения компьютерных сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в коммуникациях применяются: металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель «витая пара», коаксиальный кабель, волоконно-оптический кабель и окружающее пространство.

Линии связи, или линии передачи данных, – это промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные).

В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например, путем частотного или временного разделения каналов. Канал связи – это средство односторонней передачи данных. Если линия связи монопольно используется каналом связи, то в этом случае линию связи называют каналом связи.

Канал передачи данных – это средства двухстороннего обмена данными, которые включают в себя линии связи и аппаратуру передачи (приема) данных. Каналы передачи данных связывают между собой источники информации и приемники информации.

В зависимости от физической среды передачи данных линии связи можно разделить:

- на проводные линии связи без изолирующих и экранирующих оплеток;

- кабельные линии связи, где для передачи сигналов используются такие линии связи, как кабели «витая пара», коаксиальные кабели или оптоволоконные кабели;
- беспроводные (радиоканалы наземной и спутниковой связи), использующие для передачи сигналов электромагнитные волны, которые распространяются по эфиру.

Проводные линии связи

Проводные (воздушные) линии связи используются для передачи телефонных и телеграфных сигналов, а также для передачи компьютерных данных. Эти линии связи применяются в качестве магистральных линий связи.

По проводным линиям связи могут быть организованы аналоговые и цифровые каналы передачи данных. Скорость передачи по проводным линиям «простой старой телефонной линии» (*POST – Primitive Old Telephone System*) очень низкая. Кроме того, к недостаткам этих линий относятся чувствительность к помехам и возможность простого несанкционированного подключения к сети.

Кабельные линии связи имеют довольно сложную структуру. Кабель состоит из проводников, заключенных в несколько слоев изоляции. В компьютерных сетях используются три типа кабелей.

Витая пара (*twisted pair*) – кабель связи, который представляет собой витую пару медных проводов (или несколько пар проводов), заключенных в экранированную оболочку (рис. 12.1). Пары проводов скручиваются между собой с целью уменьшения наводок. Витая пара достаточно помехоустойчивая. Существуют два типа этого кабеля: неэкранированная витая пара *UTP* и экранированная витая пара *STP*.

Рис. 12.1. Витая пара

Характерным для этого кабеля является простота монтажа. Данный кабель – самый дешевый и распространенный вид связи, который нашел широкое применение в локальных сетях с архитектурой *Ethernet*, построенных по топологии типа «звезда». Кабель подключается к сетевым устройствам при помощи соединителя *RJ*45.

Кабель применяют при передаче данных на скоростях 10 и 100 Мб/с. Витая пара обычно используется для связи на расстоянии не более

нескольких сот метров. К недостаткам можно отнести возможность простого несанкционированного подключения к сети.

Коаксиальный кабель (*coaxial cable*) – это кабель с центральным медным проводом, который окружен слоем изолирующего материала для того, чтобы отделить центральный проводник от внешнего проводящего экрана (медной оплетки или слоя алюминиевой фольги). Внешний проводящий экран кабеля покрывается изоляцией (рис. 12.2).

Рис. 12.2. Коаксиальный кабель

Существуют два типа коаксиального кабеля: тонкий коаксиальный кабель диаметром 5 мм и толстый коаксиальный кабель диаметром 10 мм. У толстого коаксиального кабеля затухание меньше, чем у тонкого. Стоимость коаксиального кабеля выше стоимости витой пары, и выполнение монтажа сети сложнее, чем витой парой.

На концах отрезков кабеля монтируются простые *BNC*-коннекторы. Сращивание этих отрезков производят с помощью *BNC I*-коннекторов (или «баррел-коннекторов»), а для соединения с сетевыми адаптерами и устройствами используют *BNC T*-коннекторы.

Рис. 12.3. Коннекторы и терминаторы витой пары

Чтобы отраженный сигнал поглощался, на концах кабеля устанавливают *BNC*-терминаторы, один из которых обязательно заземляют (рис. 12.3).

Коаксиальный кабель применяется, например, в локальных сетях с архитектурой *Ethernet*, построенных по топологии типа «общая шина». Коаксиальный кабель более помехозащищенный, чем витая пара, и снижает собственное излучение. Пропускная способность – 50 – 100 Мб/с. Допустимая длина линии связи – несколько километров. Несанкционированное подключение к коаксиальному кабелю сложнее, чем к витой паре.

Кабельные оптоволоконные каналы связи

Оптоволоконный кабель (*fiber optic*) – это оптическое волокно на кремниевой или пластмассовой основе, заключенное в материал с низким коэффициентом преломления света, который закрыт внешней оболочкой (рис. 12.4).

Оптическое волокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон. На передающем конце оптоволоконного кабеля требуется преобразование электрического сигнала в световой, а на приемном конце – обратное преобразование.

Рис. 12.4. Оптоволоконный кабель

Существуют два различных типа оптоволоконных кабелей:

- многомодовый, или мультимодовый, кабель, более дешевый, но менее качественный;
- одномодовый кабель, более дорогой, но имеющий лучшие характеристики.

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

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего все они достигают приемника одновременно, и форма сигнала практически не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет тоже с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля.

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

Задержка распространения сигнала в оптоволоконном кабеле не сильно отличается от задержки в электрических кабелях. Типичная величина задержки для наиболее распространенных кабелей составляет 4 – 5 нс/м. Для подключения оптоволоконного кабеля используются специальные *коннекторы* (рис. 12.5). Коннекторы *FC* и *ST* сегодня считаются устаревшими, поэтому в новом оборудовании чаще всего применяются разъемы для коннекторов *SC*.

FC-коннектор *ST*-коннектор *SC*-коннектор

Рис. 12.5. Оптоволоконные коннекторы различных типов

Основное преимущество оптоволоконного кабеля – чрезвычайно высокий уровень помехозащищенности и отсутствие излучения. Несанкционированное подключение очень сложно. Скорость передачи данных 3Гб/с. Основные недостатки оптоволоконного кабеля – это сложность его монтажа, небольшая механическая прочность и чувствительность к ионизирующим излучениям.

Беспроводные каналы передачи данных (радиоканалы наземной и спутниковой связи)

Радиоканалы наземной (радиорелейной и сотовой) и спутниковой связи образуются с помощью передатчика и приемника радиоволн и относятся к технологии беспроводной передачи данных.

Радиорелейные каналы связи состоят из последовательности станций, являющихся ретрансляторами. Связь осуществляется в пределах прямой видимости, дальности между соседними станциями – до 50 км. Цифровые радиорелейные линии связи (ЦРРС) применяются в качестве региональных и местных систем связи и передачи данных, а также для связи между базовыми станциями сотовой связи.

В *спутниковых системах* используются антенны СВЧ-диапазона частот для приема радиосигналов от наземных станций и ретрансляции этих сигналов обратно на наземные станции. В спутниковых сетях

используются три основных типа спутников, которые находятся на геостационарных орбитах, средних или низких орбитах. Спутники запускаются, как правило, группами. Разнесенные друг от друга, они могут обеспечить охват почти всей поверхности Земли. Работа спутникового канала передачи данных представлена на рис. 12.6.

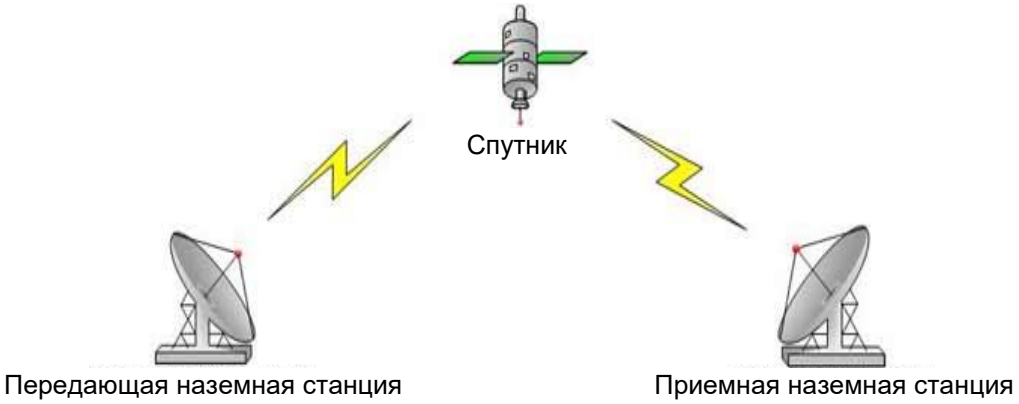


Рис. 12.6. Работа спутникового канала передачи данных

Целесообразнее использовать спутниковую связь для организации канала связи между станциями, расположенными на очень больших расстояниях, и возможности обслуживания абонентов в самых труднодоступных точках. Пропускная способность высокая – несколько десятков мегабит в секунду.

Сотовые каналы передачи данных

Радиоканалы сотовой связи строятся по тем же принципам, что и сотовые телефонные сети. Сотовая связь – это беспроводная телекоммуникационная система, состоящая из сети наземных базовых приемопередающих станций и сотового коммутатора (или центра коммутации мобильной связи).

Базовые станции подключаются к центру коммутации, который обеспечивает связь как между базовыми станциями, так и с другими телефонными сетями и глобальной сетью *Internet*. По выполняемым функциям центр коммутации аналогичен обычной АТС проводной связи.

LMDS (*Local Multipoint Distribution System*) – это стандарт сотовых сетей беспроводной передачи информации для фиксированных абонентов. Система строится по сотовому принципу, одна базовая станция позволяет охватить район радиусом несколько километров

(до 10 км) и подключить несколько тысяч абонентов. Сами базовые станции объединяются друг с другом высокоскоростными наземными каналами связи либо радиоканалами. Скорость передачи данных до 45 Мб/с.

Радиоканалы передачи данных WiMAX (*Worldwide Interoperability for Microwave Access*) аналогичны *Wi-Fi*. *WiMAX* в отличие от традиционных технологий радиодоступа работает и на отраженном сигнале, вне прямой видимости базовой станции. Эксперты считают, что мобильные сети *WiMAX* открывают гораздо более интересные перспективы для пользователей, чем фиксированный *WiMAX*, предназначенный для корпоративных заказчиков. Информацию можно передавать на расстояния до 50 км со скоростью до 70 Мб/с.

Радиоканалы передачи данных MMDS (*Multichannel Multipoint Distribution System*). Эта система способна обслуживать территорию в радиусе 50 – 60 км, при этом прямая видимость передатчика оператора является не обязательной. Средняя гарантированная скорость передачи данных составляет 500 кб/с – 1 Мб/с, но можно обеспечить до 56 Мб/с на один канал.

Радиоканалы передачи данных для локальных сетей. Стандартом беспроводной связи для локальных сетей является технология *Wi-Fi*. *Wi-Fi* обеспечивает подключение в двух режимах: точка-точка (для подключения двух ПК) и инфраструктурное соединение (для подключения нескольких ПК к одной точке доступа). Скорость обмена данными до 11 Мб/с при подключении точка-точка и до 54 Мб/с при инфраструктурном соединении.

Радиоканалы передачи данных Bluetooth – это технология передачи данных на короткие расстояния (не более 10 м) и может быть использована для создания домашних сетей. Скорость передачи данных не превышает 1 Мб/с.

12.2. Техническое обеспечение информационно-вычислительных сетей

12.2.1. Серверы и рабочие станции

Сервер *(server)* – это многопользовательский компьютер, выделенный для обработки запросов от всех рабочих станций сети, предоставляющий этим станциям доступ к общим системным ресурсам (вычислительным мощностям, базам данных, библиотекам программ, принтерам, факсам и т. д.) и распределяющий эти ресурсы.

Сервер имеет свою сетевую операционную систему, под управлением которой и происходит совместная работа всех звеньев сети. Из наиболее важных требований, предъявляемых к серверу, следует выделить высокую производительность и надежность работы.

Различают *Серверы приложений*, выполняющие содержательную обработку информации по запросам клиентов, и *Специализированные серверы,* использующиеся для устранения наиболее «узких» мест в работе сети.

Примеры специализированных серверов

1. Файл-сервер (*File Server*) – компьютер, хранящий данные пользователей сети и обеспечивающий доступ пользователей к этим данным. Как правило, это компьютер с жесткими дисками большой емкости (часто на отказоустойчивых дисковых массивах *RAID* емкостью до терабайта), со стримером и т.п. На таком компьютере обычно используется специальная операционная система, обеспечивающая одновременный доступ пользователей сети к данным, расположенным на файловом сервере. Файловый сервер выполняет следующие функции:

- хранение данных;
- архивирование данных;
- согласование изменений данных;
- передача данных.

2. Сервер прикладных программ (Application Server) – компьютер, который используется для решения прикладных программ пользователей.

3. Сервер баз данных (SQL-Server) – компьютер, выполняющий функции хранения, обработки и управления файлами баз данных. Сервер баз данных выполняет следующие функции:

- хранение, поиск и обновление записей баз данных;
- обеспечение секретности данных;
- согласование изменений данных, выполняемых разными пользователями;
- взаимодействие с другими серверами баз данных, расположенными в другом месте.

При использовании сервера баз данных пользователь на своей рабочей станции формирует запрос к серверу на выполнение какой-либо функции, например поиска записи с определенными параметрами. Далее этот запрос направляется на сервер баз данных. На сервере выполняется поиск нужной записи и передача только этой записи на рабочую

станцию. Объем передаваемой информации невелик, поэтому становится возможным использование удаленных рабочих станций. При использовании сервера баз данных снижаются требования к производительности рабочей станции, так как основная обработка данных выполняется на сервере.

4. Коммуникационный сервер (Communications Server) – устройство или компьютер, который предоставляет пользователям локальной сети прозрачный доступ к последовательным портам ввода/вывода коммуникационного сервера. С помощью коммуникационного сервера можно создать разделяемый модем, подключив его к одному из портов сервера. Пользователи, подключившись к коммуникационному серверу, могут работать с таким модемом так же, как если бы он был подключен непосредственно к рабочей станции. Некоторые коммуникационные серверы позволяют устанавливать соединение по инициативе удаленной рабочей станции, таким образом, пользователь на удаленной рабочей станции получает доступ к ресурсам локальной сети.

5. Сервер доступа (Access Server) – устройство или компьютер, позволяющий выполнять удаленную обработку заданий. Это может быть стойка, в которую устанавливаются системные платы с модемами и сетевыми платами, либо компьютер, к которому подключены модемы для связи с удаленными рабочими станциями. Обработка данных выполняется на сервере доступа. От пользователя на удаленной рабочей станции принимаются команды управления с клавиатуры, а возвращаются ему результаты выполнения заданий. Это можно сравнить с тем, что терминал и клавиатура подключены к системному блоку через телефонную линию и модемы.

6. Серверы VPN (*Virtual Private Network* – «виртуальная частная сеть») обеспечивают удаленное подключение к локальной сети по модему или через *Internet*. Это дает пользователям возможность работать с ресурсами локальной сети предприятия, офиса или учебного заведения, из дома или из любого места, где есть подключение к *Internet*, например из Интернет-кафе.

7. Терминальные серверы предоставляют возможность работы с другими серверами через специальные программы – *терминальные клиенты.* С помощью этих программ администраторы, находясь вдалеке от локальной сети, могут полностью управлять им, а пользователи – удаленно работать с установленными на сервере приложениями.

8. Сервер печати (Print Server) – устройство или компьютер, к которому подключены устройства печати, доступные пользователям сети. В настоящее время может быть реализован с помощью программного обеспечения, устанавливаемого на файловом сервере или рабочей станции, или с помощью сетевого принтера, непосредственно подключенного к локальной сети. Сервер печати выполняет следующие функции:

- позволяет пользователям сети совместно использовать устройства печати;
- обрабатывает одновременные запросы на печать, формируя для этого очереди заданий.

9. Факс-сервер (*Net SatisFaxion*) – выделенная рабочая станция для организации эффективной многоадресной факсимильной связи, с несколькими факс-модемными платами, со специальной защитой информации от несанкционированного доступа в процессе передачи, с системой хранения электронных факсов.

10. Сервер резервного копирования данных (Back Up Server) – устройство или компьютер, который решает задачи создания, хранения и восстановления копий данных, расположенных на файловых серверах и рабочих станциях. В качестве такого сервера могут использоваться один из файловых серверов сети, рабочая станция либо специализированный модуль, подключаемый непосредственно к локальной сети.

11. Архивационный сервер (сервер резервного копирования, *Storage Express System*) применяется для резервного копирования информации в крупных многосерверных сетях.

12. Почтовый сервер (*Mail Server*) – то же, что и факс-сервер, но для организации электронной почты с электронными почтовыми ящиками.

13. Серверы-шлюзы (Proxy-серверы). Классический прокси-сервер поддерживает функцию буфера для временного хранения передаваемых данных, так что при повторном запросе данных, еще хранимых на сервере, их не нужно искать снова, а можно прямо воспользоваться хранимой копией. Более того, если связь с сетью прервется, прокси-сервер будет продолжать работать.

В *Internet* прокси-серверы исполняют роль маршрутизаторов, почти всегда совмещенную с функциями почтового сервера и *сетевого*

брандмауэра, обеспечивающего безопасность внутри сетевой информации. Но брандмауэр с фильтрацией пакетов функционирует на сетевом уровне модели *OSI*, а *proxy*-серверы работают на прикладном уровне. Они разрывают прямое соединение между клиентом и сервером, при этом все внутренние *IP*-адреса сети отображаются на единственный «надежный» *IP*-адрес.

14. Веб- и FTP-серверы предоставляют для внешних (а часто и для внутренних) пользователей доступ к веб- и *FTP*-ресурсам, размещенным в данной сети.

15. Контроллеры домена обеспечивают в сетях *Microsoft* работу служб *Активного каталога* (*Active Directory*) и поддерживают базу данных всех зарегистрированных в *домене* пользователей, компьютеров, групп и ресурсов. Наличие такой базы данных позволяет администраторам централизованно управлять всеми сетевыми объектами и ресурсами. Пользователи же получают возможность входить в сеть с любого принадлежащего домену компьютера, а затем «прозрачно» (без ввода имени и пароля) подключаться к другим ПК и работать с их ресурсами.

Этот список далеко не полон, существуют и другие типы серверов.

Рабочая станция *(work station)* сети на базе обычного компьютера функционирует как в сетевом, так и локальном режимах. Она оснащена собственной операционной системой и обеспечивает пользователя всем необходимым для решения прикладных задач.

Рабочие станции иногда специализируются для выполнения графических, инженерных, издательских и других работ. В этом случае они должны строиться на базе мощного компьютера, имеющего два процессора, емкий и быстродействующий винчестер на интерфейсе *SCSI*, монитор с большим экраном (а иногда и оснащенные соответствующей графической платой два монитора, например, один для отображения проекта, а второй для отображения меню или сообщений электронной почты).

Рабочие станции на базе сетевых компьютеров могут функционировать, как правило, только в сетевом режиме при наличии в сети сервера приложений.

Отличие *сетевого компьютера* (*Network Personal Computer – NET PC*) от обычного в том, что он максимально упрощен: классический *NET PC* не содержит дисковой памяти (часто называют бездисковым ПК). Он имеет упрощенную материнскую плату, основную память, а из внешних устройств – только дисплей, клавиатуру, мышь и сетевую карту обязательно с чипом ПЗУ *BootROM*, обеспечивающим возможность удаленной загрузки операционной системы с сервера сети (это классический «тонкий клиент» сети). Для работы, например, в сети Интранет такой компьютер должен иметь столько вычислительных ресурсов, сколько требует *Internet*-браузер.

Хост-компьютеры – это компьютеры, имеющие непосредственный доступ в глобальную сеть.

12.2.2. Концентраторы, приемопередатчики и повторители

Сетевой концентратор, или *хаб* (от англ. *hub* – центр), – устройство для объединения компьютеров в сеть с применением кабельной инфраструктуры типа *витая пара* (рис. 12.7).

Рис. 12.7. Сетевой концентратор

Концентратор работает на физическом уровне сетевой модели *OSI*, повторяет приходящий на один порт сигнал на все активные порты. В случае поступления сигнала на два и более порта одновременно возникает коллизия, и передаваемые кадры данных теряются. Таким образом, все подключённые к концентратору устройства находятся в одном домене коллизий. Концентраторы всегда работают в режиме полудуплекса, все подключённые устройства *Ethernet* разделяют между собой предоставляемую полосу доступа.

Многие модели концентраторов имеют простейшую защиту от излишнего количества коллизий, возникающих по причине одного из подключённых устройств. В этом случае они могут изолировать порт от общей среды передачи. По этой причине сетевые сегменты, основанные на витой паре, гораздо стабильнее в работе сегментов на коаксиальном кабеле, поскольку в первом случае каждое устройство может быть изолировано концентратором от общей среды, а во втором случае

несколько устройств подключаются при помощи одного сегмента кабеля, и в случае большого количества коллизий концентратор может изолировать лишь весь сегмент.

В последнее время концентраторы используются достаточно редко, вместо них получили распространение коммутаторы – устройства, работающие на канальном уровне модели *OSI* и повышающие производительность сети путём логического выделения каждого подключённого устройства в отдельный сегмент, домен коллизии. Сетевые коммутаторы ошибочно называют «интеллектуальными концентраторами».

Приемопередатчик (трансивер) – это устройство, предназначенное для приема пакетов от контроллера рабочих станций сети и передачи их в шину. Он также разрешает коллизии в шине. Конструктивно приемопередатчик и контроллер могут объединяться на одной плате или находиться в различных узлах.

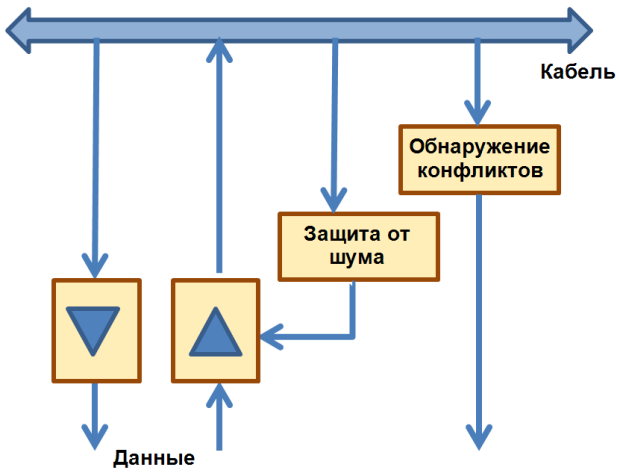


Рис. 12.8. Блок-схема приемопередатчика

В состав приемопередатчика в магистральные ЛВС входят (рис. 12.8):

- *приемник сигналов* от линии передачи данных; его назначение – усиление информационных сигналов и обнаружение конфликтов путем выделения постоянной составляющей искаженных сигналов и ее сопоставления в компараторе с эталонным напряжением;
- *передатчик* от станции в линию;
- *ответвитель* для подсоединения входов приемника и выходов передатчика к кабелю; применяется механическое контактирующее устройство, накладываемое на кабель и имеющее винт-иглу, которой прокалывается оплетка кабеля и осуществляется контакт с центральным проводником; игольчатый контакт имеет трансформаторную связь с приемником и передатчиком сигналов;

• *защита от шума* для отключения источника данных от кабеля, при ошибочной генерации сигналов дольше, чем это предусмотрено.

Приемопередатчик (повторитель) для волоконно-оптических линий передачи данных (световодов) также включает части приемную, передающую, чтения и записи данных. В приемной части имеются фотодиод, усилитель-формирователь сигналов с требуемыми уровнями напряжения, механическое контактирующее устройство для надежного контакта фотодиода со стеклянной оболочкой кабеля. Передатчик представлен светодиодом или микролазером.

Рис. 12.9. Сетевой повторитель

Повторитель (репитер) – устройство с автономным питанием, обеспечивающее передачу данных между сегментами определенной длины (рис. 12.9). Так как он, по сути, является усилителем электрического сигнала, то в нем не выполняется никаких обработок и изменений передаваемой информации. Повторитель воспринимает входные импульсы, удаляет шумовые сигналы и передает вновь сформированные пакеты в следующий кабельный сегмент или сегменты. Никакого редактирования или анализа поступающих данных не производится. Задержка сигнала повторителем не должна превышать 7,5 тактов (750 нс для обычного *Ethernet*). Схема сетевого повторителя приведена на рис. 12.10. Повторители могут иметь коаксиальные входы/выходы, *AUI*-разъемы для подключения трансиверов или других аналогичных устройств, или каналы для работы со скрученными парами.

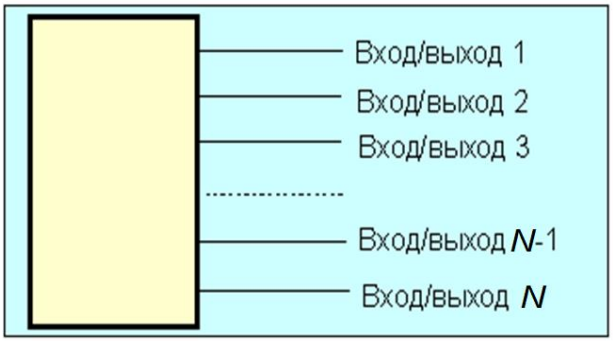


Рис. 12.10. Схема сетевого повторителя

Все входы/выходы повторителя с точки зрения пакетов эквивалентны. Если повторитель многовходовый, то пакет, пришедший по

любому из входов, будет ретранслирован на все остальные входы/выходы повторителя.

12.2.3. Мосты, маршрутизаторы, коммутаторы и шлюзы

Сетевой мост *(bridge)* представляет собой репитер, усиленный функциями анализа и обработки передаваемых данных, и используется при объединении кабельных сегментов.

Функция анализа заключается в следующем: мост собирает сведения о том, какие устройства к каким портам подключены по их адресам управления доступом к среде (*Media Access Control – MAC*-адреса); мост заносит эти адреса в свою таблицу, и в дальнейшем может использовать для переадресации входных кадров только тому порту, который является его получателем.

Мост имеет два или более портов, работает на канальном уровне, осуществляет отбор передаваемых через него пакетов и обеспечивает функции фильтрации пакетов. Алгоритм фильтрации: у каждого полученного пакета считывается адрес получателя из заголовка протокола канального уровня. Если пакет предназначен для узла другого сегмента, то он передается в этот сегмент, если пакет предназначен узлу в локальном сегменте, то мост обрабатывает его, поскольку это сообщение уже достигло адресата.

Различают три типа мостов:

1) *локальные*, обеспечивающие фильтрацию пакетов и ретранслирующие услуги для сегментов одинакового типа, их называют мосты *MAC*-уровня;

2) *преобразующие*, обеспечивающие функции локального моста с дополнительной возможностью работы с разными протоколами и скоростями;

3) *удаленные*, когда мост соединяет сетевые сегменты, расположенные на значительном расстоянии друг от друга, используя соединения глобальной сети (модем, выделенная линия). Работает медленнее, чем локальный и преобразующий, но стоит дороже.

Структура моста показана на рис. 12.11.

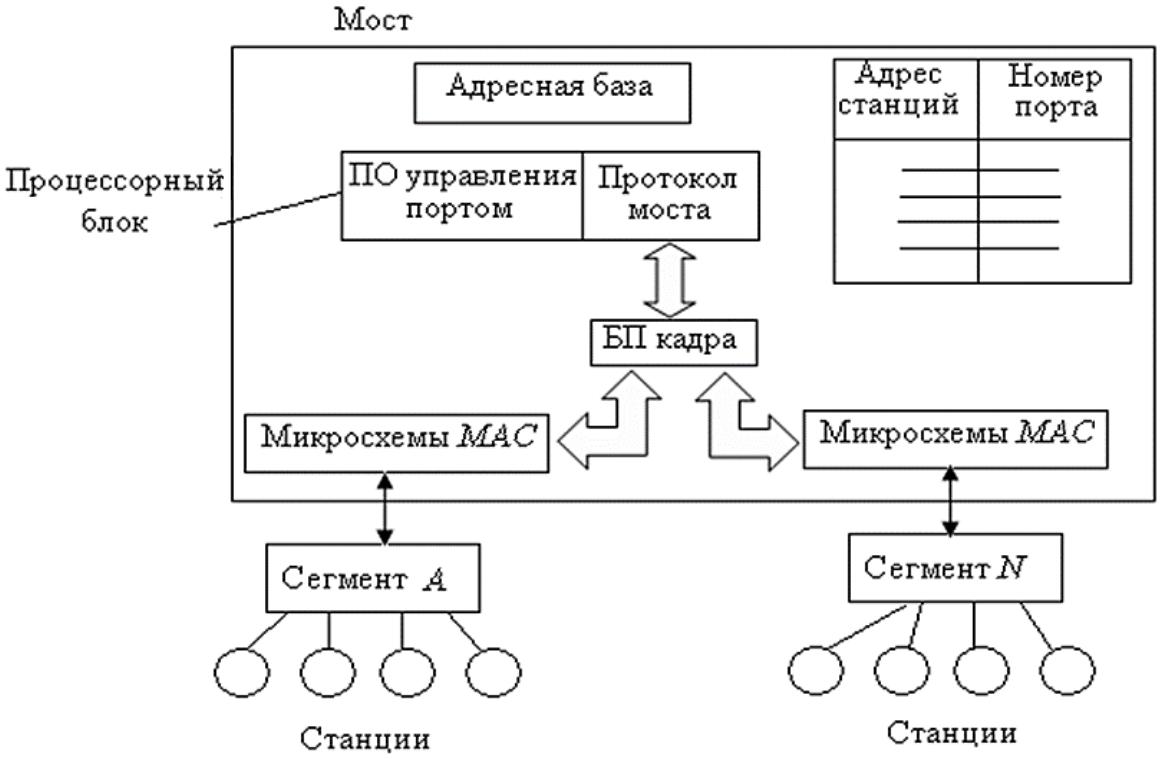


Рис. 12.11. Структура моста: БП – буферная память, в которой хранятся кадры

Поскольку вначале при организации ЛВС мост не содержит никаких сведений о ее структуре, то необходимо, чтобы мост обладал способностью «самообучения». Процесс обучения моста происходит по следующему сценарию (рис. 12.12):

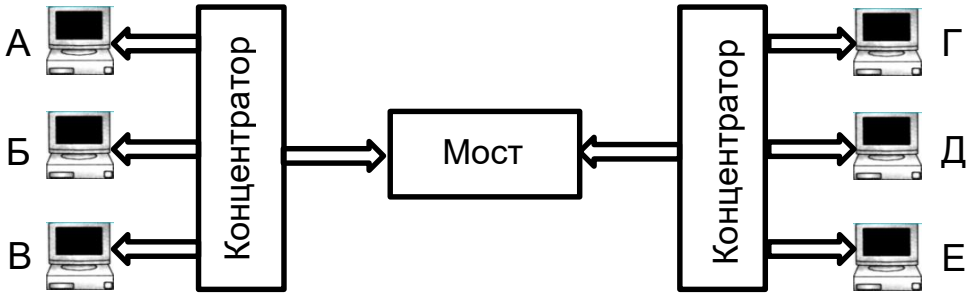


Рис. 12.12. Схема процесса обучения моста

При посылке пакета со станции *A* к *B* концентратор повторяет кадр всем своим портам, один из которых подключен к мосту. Мост создает запись в своей таблице и передает сообщение на противоположный порт, поскольку не знает, в каком сегменте находится станция *B*.

Станция *B* обнаруживает, что кадр адресован ей и начинается сеанс связи. Однако, как только мост фиксирует пакет от рабочей станции *B* к станции *A*, он уже не повторяет кадр другому порту, так как ему известно, что станции *A* и *B* принадлежат одному и тому же сегменту.

По мере расширения сети мост «обучается» и узнает о всех *MAC*-адресах рабочих станций в сегментах, к которым он подключен.

Маршрутизаторы (роутеры) и шлюзы устанавливают соединение на 3-м и 4-м уровнях, при этом верхние уровни сети (5-й, 6-й и 7-й) должны быть одинаковые. Они обеспечивают достаточно сложный уровень сервиса, так как могут выполнять «интеллектуальные» функции: выбор наилучшего маршрута для передачи сообщения, адресованного другой сети; управление сбалансированной нагрузкой в сети путем равномерного распределения потоков данных; защиту данных; буферизацию передаваемых данных; различные протокольные преобразования. Такие возможности маршрутизаторов особенно важны при построении базовых сетей крупных организаций.

Маршрутиза́тор (*router*) – специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

Маршрутизатор работает на более высоком «сетевом» уровне сетевой модели *OSI*, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают соответственно на 2-м и 1-м уровнях модели *OSI*.

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из некоторого числа записей – маршрутов, в каждом из которых содержится адрес сети получателя, адрес следующего узла, которому следует передавать пакеты, административное расстояние – степень доверия к источнику маршрута и некоторый вес записи – метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям.

Уровень передачи пакетов маршрутизации реализуется на алгоритмах коммутации и, как правило, одинаков для большинства прото-

колов. Промежуточный маршрутизатор, имея адрес следующего маршрутизатора, посылает ему пакет, адресованный специально на физический адрес (*MAC*-уровень) этого маршрутизатора, но с адресом (сетевого уровня) получателя.

По адресу получателя маршрутизатор определяет, знает ли он, как передать пакет следующему маршрутизатору в пути. Если знает, то пакет отсылается следующему маршрутизатору путем замены физического адреса получателя на физический адрес следующего маршрутизатора. Если маршрутизатор не знает, то пакет игнорируется. На следующем маршрутизаторе все повторяется. По мере прохождения пакета через сеть его физический адрес меняется, но адрес сетевого уровня остается неизменным. Этот процесс проиллюстрирован на рис. 12.13.

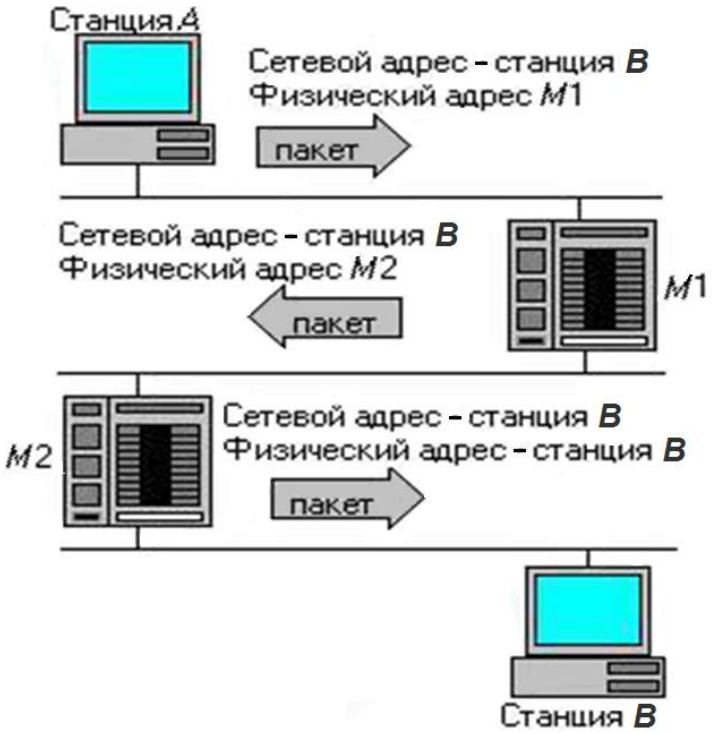


Рис. 12.13. Схема процесса передачи пакетов
при маршрутизации

Существуют два типа протоколов для маршрутизаторов: *внутренние и внешние*.

Внутренние протоколы (*Interior GateWay Protocol – IGP*) выполняют функции маршрутизации в автономных сетях (связь типа «узел»).

Внешние протоколы (*Exterior GateWay Protocol – EGP*) маршрутизации (связь типа «маршрутизатор – маршрутизатор») отвечают за маршрутизацию между автономными сетями и *Internet.*

Шлюзы – это устройства, функционирующие как маршрутизатор, но, кроме того, выполняющие некоторые функции по передаче данных между двумя различными сетями с помощью сетевых протоколов. Сетевым шлюзом (*networking gateway*, или просто *gateway*) называют аппаратное или программное обеспечение либо их комбинацию, выполняющую передачу данных между несовместимыми прикладными программами или между сетями, использующими различные протоколы.

Подобно шлюзам на космическом корабле или на подводной лодке, которые обеспечивают безопасный переход из одной физической среды в другую, сетевые шлюзы обеспечивают передачу информации из одной сети в другую. Если эти сети оказываются гетерогенными, то информацию недостаточно просто передать, ее необходимо преобразовать к виду, используемому в сети, куда эта информация направляется.

Обычно сетевым шлюзом называют устройство, объединяющее, прежде всего, именно разнородные сети или системы, для обеспечения взаимодействия которых требуется преобразование передаваемой информации.

Например, сетевыми шлюзами третьего, или сетевого, уровня называют маршрутизаторы, объединяющие две или больше сетей и способные согласовать их работу, т. е. обеспечить «шлюзование» передаваемой между сетями информации – преобразование поступающих из одной сети пакетов в пакеты, совместимые с другой сетью и способные в ней обращаться.

Сетевыми шлюзами прикладного уровня модели *OSI* называют прокси-серверы (*proxy-server*, от англ. *proxy* – уполномоченный, заместитель, доверенное лицо, передача полномочий).

Прокси-сервер – отдельный узел сети с установленным на нем программным обеспечением, который специализируется на обработке запросов пользовательских приложений, направленных серверам, расположенным в сети, а также сохраняет полученные на эти запросы ответы, что позволяет при повторном запросе выдать пользователю ответ

немедленно, не дожидаясь прихода результата с сервера внешней сети. Все потоки информации от приложений до запрашиваемых ими серверов проходят через прокси-сервер.

Они выполняют протокольное преобразование для всех семи уровней модели ВОС, в частности, маршрутизацию пакетов, преобразование сообщения из одного формата в другой или из одной системы кодирования в другую.

Сетевой коммутатор (*switch* – переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети (рис. 12.14). Коммутатор работает на канальном (втором) уровне модели *OSI*. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.

Рис. 12.14. Сетевой коммутатор

В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых не известен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор хранит в памяти таблицу коммутации (хранящуюся в ассоциативной памяти), в которой указывается соответствие *MAC*-адреса (т.е. уникального идентификатора, присваиваемого каждой единице активного оборудования компьютерных сетей узла) порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора, коммутатор анализирует фреймы (кадры) и, определив *MAC*-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, *MAC*-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если *MAC*-адрес хоста-

получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных *MAC*-адресов, в результате трафик локализуется.

Коммутаторы подразделяются на управляемые и неуправляемые (наиболее простые).

Более сложные коммутаторы позволяют управлять коммутацией на высших уровнях модели *OSI*. Обычно их именуют соответственно, например, «*Layer* 2 *Switch*», или сокращенно «*L*2 *Switch*».

Коммутаторы уровня 2 работают на втором (канальном) уровне модели *OSI*. Они решают две основные задачи:

- проверка входящего трафика;
- отслеживание физических адресов всех станций, подключенных к их портам, и пересылка трафика по конкретным адресам в соответствии со встроенной в них таблицей пересылки.

Такие коммутаторы обладают высоким быстродействием, потому что не проверяют индивидуальные пакеты данных, а просто передают их дальше.

Коммутаторы уровня 3, называемые также маршрутизирующими коммутаторами (реже – коммутирующими маршрутизаторами и иногда даже *IP*-коммутаторами), выполняют одновременно функции и коммутации, и маршрутизации. Они работают на третьем, или сетевом, уровне модели *OSI*, который содержит в частности *IP*-адреса. Такие коммутаторы основываются на использовании специализированных интегральных микросхем и специализированных «коммутирующих фабрик». Кроме того, в них применяются быстродействующие центральные процессоры (ЦП) и другие компоненты, что и позволяет достичь высокой скорости маршрутизации. Коммутаторы уровня 3 могут служить для замены унаследованных сетевых маршрутизаторов, повышая интенсивность коммутируемого трафика (по сравнению с традиционными маршрутизаторами) в 10 раз.

Коммутаторы уровня 4. Наиболее продвинутые коммутаторы уровня 3 позволяют производить одновременную фильтрацию для уровней 2, 3 и 4 и даже выше, что помогает гарантировать доставку критически важных данных до нужного пункта без замедления работы сети. Добавление функциональности уровня 4 при этом позволяет

управлять трафиком. Целесообразность совмещения функций, реализуемых на четвертом уровне, с функциями коммутации и маршрутизации (уровни 2 и 3) связана с тем, что для предотвращения перегрузок в сети может оказаться полезной способность системы анализировать информацию транспортного и более высоких уровней. Поэтому правильнее было бы называть коммутаторы уровней выше третьего «зависимыми от приложения».

Gigabit Ethernet коммутаторы занимают особое место среди коммутаторов верхних уровней, которые на самом деле представляют собой технологический прорыв. Именно такие коммутаторы наиболее интересны для развивающихся компаний.

Они предназначены в основном для использования в качестве коммутаторов опорной сети предприятия и средства организации высокоскоростных каналов с гигабитными скоростями по медной среде и оптическому волокну.

Уровень 4 – не самый верхний, на котором работают современные коммутаторы. Например, компания *VIPswitch* предлагает продукты, позиционируемые ею как коммутаторы уровня 5. Эти многопортовые полнодуплексные коммутаторы с функцией обеспечения качества обслуживания без блокирования служат для передачи видео, голоса и данных. Они позволяют пользователям высокоэффективно передавать мультимедийные потоки в режиме реального времени.

А компания *Top Layer Networks* предлагает продукт *AppSwitch* 2000, позиционируемый ею как коммутатор уровня 7. Как утверждают его создатели, он позволяет «сортировать» трафик по приложениям или даже по самим пользователям в соответствии с предопределенными политиками. Он содержит мастер настройки, который помогает *IT*-менеджерам 90 % пропускной способности выделить клиентским приложениям, а 10 % оставить для служебных нужд.

Многие управляемые коммутаторы позволяют настраивать дополнительные функции: *VLAN, QoS*, агрегирование, зеркалирование.

Сложные коммутаторы можно объединять в одно логическое устройство – стек с целью увеличения числа портов. Например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с 90 ($(4 \cdot 24) – 6 = 90$) либо с 96 портами (если для стекирования используются специальные порты).

По своему назначению и функциональным возможностям современные мосты, маршрутизаторы и коммутаторы довольно близки друг к другу. Однако каждый из типов этих устройств разрабатывался не с целью вытеснения других устройств, он имеет свои области применения. *Мосты* обеспечивают сегментацию сети на физическом уровне, поэтому их «интеллектуальные» возможности ограничены. *Маршрутизаторы*, интегрируя физические и логические сегменты сети в единое целое, решают при этом ряд «интеллектуальных» функций, но отличаются невысоким быстродействием. *Коммутаторы* идеально приспособлены для поддержки высокопроизводительной коллективной работы.

При формировании больших сетей масштаба предприятия наиболее удачен комбинированный вариант использования мостов, маршрутизаторов и коммутаторов, умелое их сочетание, позволяющее создать действительно гибкую сетевую архитектуру.

Лучшим способом для понимания отличий между сетевыми адаптерами, повторителями, мостами/коммутаторами и маршрутизаторами является рассмотрение их работы в терминах модели *OSI*. Соотношение между функциями этих устройств и уровнями модели *OSI* показано на рис. 12.15.

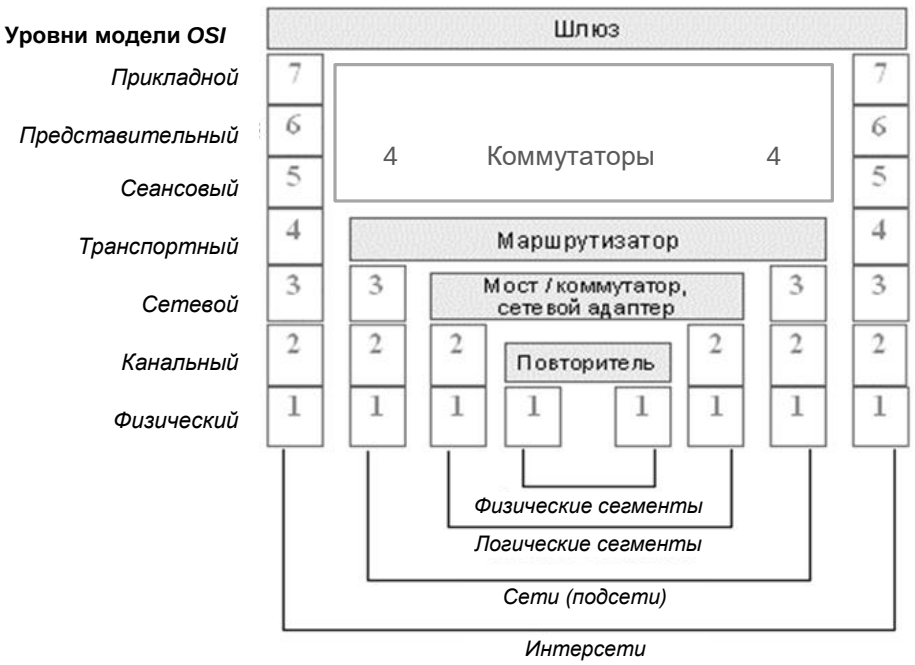


Рис. 12.15. Соотношение функций сетевых устройств и уровней модели *OSI*

Повторитель, который регенерирует сигналы, за счет чего позволяет увеличивать длину сети, работает на физическом уровне.

Сетевой адаптер работает на физическом и канальном уровнях. К физическому уровню относится та часть функций сетевого адаптера, которая связана с приемом и передачей сигналов по линии связи, а получение доступа к разделяемой среде передачи, распознавание *MAC*-адреса компьютера – это уже функция канального уровня.

Мосты выполняют большую часть своей работы на канальном уровне. Для них сеть представляется набором *MAC*-адресов устройств. Они извлекают эти адреса из заголовков, добавленных к пакетам на канальном уровне, и используют их во время обработки пакетов для принятия решения о том, на какой порт отправить тот или иной пакет. Мосты не имеют доступа к информации об адресах сетей, относящейся к более высокому уровню. Поэтому они ограничены в принятии решений о возможных путях или маршрутах перемещения пакетов по сети.

Маршрутизаторы работают на сетевом уровне модели *OSI*. Для маршрутизаторов сеть – это набор сетевых адресов устройств и множество сетевых путей. Маршрутизаторы анализируют все возможные пути между любыми двумя узлами сети и выбирают самый короткий из них. При выборе могут приниматься во внимание и другие факторы, например, состояние промежуточных узлов и линий связи, пропускная способность линий или стоимость передачи данных.

12.2.4. Модемы и факс-модемы

Модем (МОдулятор-ДЕМодулятор) – это устройство, позволяющее обмениваться информацией *PC* (т.е. цифровых устройств), через аналоговые каналы (обыкновенные телефонные станции и сети).

Назначение модема заключается в замене цифрового сигнала, поступающего из *PC*, электрическим сигналом с частотой, соответствующей рабочему диапазону телефонной линии (рис. 12.16).

Рис. 12.16. Схема передачи сигнала с аналого-цифровым преобразованием

Акустический канал этой линии модем разделяет на две полосы низкой и высокой частоты. Полоса низкой частоты применяется для передачи данных, а полоса высокой частоты – для приема. Используются три способа кодировки информации:

• метод *FSK* (*Frequency Shift Keying* – частотный) для скорости передачи до 300 бод (бит/с);

• метод *PSK* (*Phase Shift Keying* – фазовый) для более быстрых модемов;

• квадратурно-амплитудный метод – *QAM* (*Quadrature Amplitude Modulation*), при котором в такт передаваемым данным изменяются одновременно и фаза, и амплитуда сигнала.

В данное время существуют модемы, способные передавать со скоростью более 56 000 бод.

При частотном методе сигнал «1» передается на частоте большей, чем сигнал «0».

Метод *PSK* использует всего две частоты: для передачи данных – 2400 Гц и для приема – 1200 Гц.

Фазовое соотношение

Сочетание бит	Сдвиг фазы (градус)
00	0
01	90
10	180
11	270

Данные передаются по два бита, при этом кодировка осуществляется посредством сдвига фазы сигнала (см. таблицу).

Модем выполняется либо в виде внешнего устройства, которое одним выходом подсоединяется к телефонной линии, а другим – к *PC* через последовательный асинхронный адаптер (например, *RS*-232-*C* или др.), либо в виде платы (внутренний модем), которая устанавливается на общую шину *PC* (в слот материнской платы). Внешний модем проще в установке и имеет больше возможностей для контроля и настройки благодаря расположению и наличию светодиодных индикаторов (*LED*). Преимущество внутреннего модема заключается в цене и в том, что на рабочем месте оператора нет дополнительного периферийного устройства.

Типичный модем содержит следующие компоненты: специализированный микропроцессор, управляющий работой модема, оперативную память, хранящую значения регистров модема и буферизующую входную/выходную информацию, постоянную память, динамик, позволяющий выполнять звуковой контроль связи, а также другие вспо-

могательные элементы (трансформатор, резисторы, конденсаторы, разъемы). Современные модемы дополнительно содержат электрически перепрограммируемую постоянную память, в которой может быть сохранена конфигурация модема даже при выключении питания.

На плате модема имеются конфигурационные переключатели (свитчи), которые позволяют устанавливать некоторые параметры модема. Как правило, свитчами устанавливается адрес порта модема (*COM*1 – *COM*4).

Другие параметры модема могут устанавливаться также переключателями типа *JAMPER* (джампер), расположенными на его плате.

Различают следующие режимы работы модема:

1) режим передачи данных, в котором модем передает и принимает данные;

2) режим команд, с помощью которых можно программировать работу модема.

Для режима команд нормой признан так называемый набор команд *Hayes* (фирма *Hayes*), состоящий из *AT*-команд и обеспечивающий всем модемам единую основу для осуществления связи друг с другом. Эти команды (за некоторым исключением) начинаются с префикса *AT* (*Attention* – внимание), который дополняется собственно командой с параметрами. Например, команда A*TDP*8*W*095100 означает вызов (команда *DP*) абонента из Москвы (код 8, ожидание гудка, 095) по номеру 100.

Существуют также два режима передачи команд *PC* и ответов модема: асинхронный и синхронный.

В *асинхронном* режиме формат передаваемой команды состоит из стартового бита, 8 битов данных и стоп-бита. В состав битов данных входит 1 бит проверки на четность.

В *синхронном* режиме стартовый бит и стоп-бит не передаются. Передача информации осуществляется в виде так называемых кадров, в состав которых входят заголовок, поле информации и комбинация проверки. В настоящее время в модемах, как правило, используется синхронный режим.

Передача данных на большие расстояния, как правило, подвержена ошибкам. Для решения таких проблем разработаны методы коррекции ошибок, которые вместе с методами сжатия данных определяются соответствующими протоколами.

Протоколом организации сети *PC* является *Microcom Networking Protocol-MNP*. *MNP*-коррекция может быть реализована или аппаратно

(все современные модемы имеют встроенные протоколы коррекции ошибок), или на программном уровне с помощью телекоммуникационного пакета (ТП), входящего в *Windows*.

Принцип работы *MNP*-модема заключается в использовании при передаче информации блоков переменной длины. Модем принимает от компьютера подлежащие передаче данные и собирает их в пакет (блок), который затем передается. При этом вычисляется контрольная сумма, которая передается в конце пакета. При ошибочной передаче в случае несовпадения объема переданной информации и контрольной суммы модем на принимающей стороне затребует повтора передачи неправильно переданного блока.

При передаче важных данных (исполняемого кода архивированных данных и т.п.) ошибка даже в одном бите может привести к полной потере информации. Поэтому для надежного обмена файлами созданы различные алгоритмы передачи данных, соответствующие определенным стандартам передачи сигналов.

Первый стандарт определяет скорости передачи данных – разработаны модемы стандартов *V*.32 для скорости 9600 бит/с, *V*.32 *bis* для 14400 бит/с, *V*.92 для 56000 бит/с и т.д. В более скоростных модемах обычно реализованы и предшествующие стандарты передачи сигналов и, кроме того, предусмотрены запасные режимы с меньшими скоростями. Например, для стандарта *V*.32 *bis* – это скорости 12000, 9600, 7200 и 4800 бит/с.

Второй стандарт связан с используемыми протоколами коррекции ошибок. Многие годы стандартом считались протоколы группы *MNP* (*Microcom Networking Protocol*) – *MNP*1–*MNP*10. Это аппаратные протоколы фирмы *Microcom*, обеспечивающие автоматическую коррекцию ошибок и компрессию (сжатие) передаваемых данных. В настоящее время используется стандарт МККТТ *V*.42 (Международный консультативный комитет по телеграфии и телефонии). Комитет недавно переименован в Международный институт телекоммуникаций (*ITU – International Telecommunication Union*). В целях совместимости модем стандарта *V*.42 включает в себя и функции *MNP*.

Третий стандарт определяет реализуемый метод сжатия данных. Здесь также стандарт *MNP*5, предусматривающий сжатие информации всего лишь вдвое, уступает место стандарту Международного комитета по телеграфии и телефонии (МККТТ) *V*.42 *bis*, выполняющему сжатие информации в четыре раза.

Факс-модемы обеспечивают скоростную передачу данных только в одном направлении и используют свои собственные стандарты. Они лучше справляются с передачей информации, чем с приемом. В настоящее время выпускаются и комбинированные модемы (модем данных/факс-модем).

Модемы для цифровых каналов связи

Цифровые модемы более правильно называть сетевыми адаптерами, ибо о классической модуляции-демодуляции сигналов в них речи не идет – входной и выходной сигналы такого модема являются импульсными.

Цифровые модемы выпускаются для работы в конкретных цифровых технологиях: *ISDN, HDSL, ADSL, SDSL* и т. д.

Различают:

• *кабельные модемы* для работы с сетями через коммуникации кабельного телевидения, например, они обеспечивают скорость передачи данных в среднем до 36 Мб/с и принимают со скоростью до 2 Мб/с;

• *сотовые модемы* для работы в системе сотовой телефонной связи. Это обычно *PCMCIA*-модемы для работы в стандартах *GSM, CDMA*;

• *оптоволоконные модемы* для работы по волоконно-оптическим каналам связи по протоколам *FDDI*;

• *спутниковые радиомодемы* для приема данных через спутник: прием информации осуществляется через спутниковую антенну со скоростями до 400 кб/с, а передача возможна только при наличии громоздкого дорогостоящего оборудования;

• *силовые модемы* для работы в сетях через систему электропитания компьютеров.

12.2.5. Сетевые адаптеры и анализаторы

Сетевые адаптеры *(сетевые карты, network adapter, net card)* обеспечивают физическую связь системы и передающей физической среды.

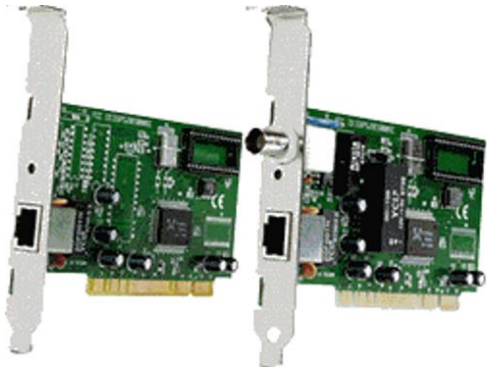


Рис. 12.17. Общий вид плат сетевого адаптера

Сетевые адаптеры (СА) предназначены для сопряжения сетевых устройств со средой передачи в соответствии с принятыми правилами обмена информацией (рис. 12.17).

Сетевым устройством может быть компьютер пользователя, сетевой сервер, рабочая станция и т. д. Набор выполняемых сетевым

адаптером функций зависит от конкретного сетевого протокола и может перераспределяться между адаптером и компьютером. Чем больше функций выполняет компьютер, тем проще функциональная схема адаптера. К основным сетевым функциям адаптера относятся:

- гальваническая развязка с коаксиальным кабелем или витой парой. Наиболее часто для этой цели применяют импульсные трансформаторы, иногда – оптроны;
- кодирование и декодирование сигналов. Наиболее часто применяется самосинхронизирующийся манчестерский код;
- идентификация своего адреса в принимаемом пакете. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ;
- преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме. В простейшем случае для этой цели используются сдвиговые регистры с параллельным входом и последовательным выходом. Эта функция может быть реализована и программными методами;
- промежуточное хранение данных и служебной информации в буфере;
- выявление конфликтных ситуаций и контроль состояния сети;
- подсчет контрольной суммы;
- согласование скоростей пересылки данных компьютером в адаптер или из него со скоростью обмена по сети.

Указанные выше основные функции адаптеров и их технические характеристики определяются поддерживаемым уровнем протокола ЛКС в соответствии с архитектурой семиуровневой эталонной модели ВОС.

По выполняемым функциям СА разделяются на две группы:

1. Реализующие функции физического и канального уровней.

Такие адаптеры, выполняемые в виде интерфейсных плат, отличаются технической простотой и невысокой стоимостью. Они применяются в сетях с простой топологией, где практически отсутствует необходимость выполнения таких функций, как маршрутизация пакетов, формирование из поступающих пакетов сообщений, согласование протоколов различных сетей и др.

2. Реализующие функции первых четырех уровней модели ВОС – физического, канального, сетевого и транспортного. Эти адаптеры, кроме функций СА первой группы, могут выполнять функции маршрутизации, ретрансляции данных, формирования пакетов из передаваемого сообщения (при передаче), сборки пакетов в сообщение (при приеме), согласования ПДД различных сетей, сокращая таким образом затраты вычислительных ресурсов ЭВМ на организацию сетевого обмена. Технически они могут быть выполнены на базе микропроцессоров. Естественно, что такие адаптеры применяются в ЛКС, где имеется необходимость в реализации перечисленных функций.

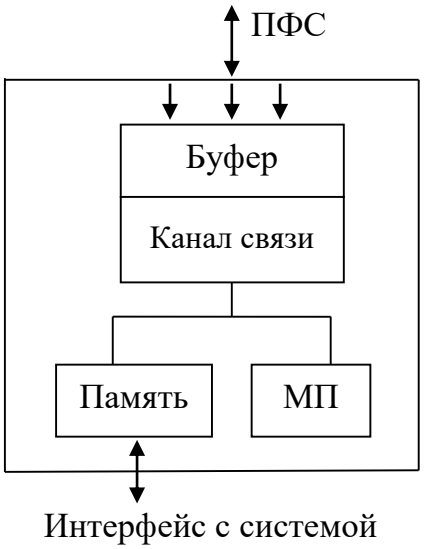


Рис. 12.18. Обобщенная структура сетевого адаптера

Обобщенная структура сетевого адаптера представлена на рис. 12.18).

СА содержит один или более каналов прямого доступа к памяти (*Direct Memory Access – DMA*), используемых для обмена данными между передающей физической средой ПФС и памятью СА.

МП – микропроцессор, управляет работой памяти, каналами и взаимодействием с системами. СА содержит схемы, необходимые для приема/передачи данных из/в ПФС и память, используемую для буферизации входных/выходных информационных кадров.

При приеме кадра он поступает в буфер, где производится сравнение адреса назначения кадра с адресом сетевого адаптера. Если адреса совпадают, то кадр пересылается в память по одному из каналов, который инициализирован процессором. В конце каждой операции пересылки генерируется прерывание процессора. При обработке этого прерывания выполняется поиск свободного приемного буфера, после чего инициализируется канал *DMA* для приема данных в найденный буфер. При передаче данных от системы данные заносятся в память.

Поскольку адаптеры ориентированы на определенную архитектуру локальной сети и ее технические характеристики, то по топологии ЛКС адаптеры разделяются на следующие группы: поддерживающие шинную топологию, кольцевую, звездообразную, древовидную, комбинированную (звездно-кольцевую, звездно-шинную).

Сетевые адаптеры можно разделить еще на две группы:

- адаптеры для клиентских компьютеров;
- адаптеры для серверов.

В адаптерах для клиентских компьютеров значительная часть работы по приему и передаче сообщений перекладывается на программу, выполняемую в ПК. Такой адаптер проще и дешевле, но он дополнительно загружает центральный процессор машины.

Адаптеры для серверов снабжаются собственными процессорами, организующими всю нужную работу.

СА выполняются в виде плат расширения, устанавливаемых в разъем материнской платы. Еще есть карты, вставляемые в разъем *ISA*, но современные устанавливаются обычно в разъем *PCI*. Для портативных компьютеров имеются *PCMCIA*-адаптеры, а также сетевые адаптеры и для интерфейса *USB*.

Основные характеристики адаптеров:

1) установленная микросхема контроллера (микрочипа);

2) разрядность – 8-, 16-, 32- и 64-битные сетевые карты (определяется микрочипом);

3) скорость передачи – от 10 до 1000 Мб/с (наиболее популярные 10 и 100 Мб/с);

4) тип подключаемого кабеля – коаксиальный кабель толстый и тонкий, неэкранированная витая пара, волоконно-оптический кабель;

5) поддерживаемые стандарты передачи данных – *Ethernet, IEEE* 802.3*, Token Ring, FDDI* и т. д.

Анализаторы ЛКС – это мощный диагностический инструмент, предназначенный для контроля качества функционирования сети. Контроль позволяет наблюдать за работой сети в режиме реального времени и регистрировать события, которые могут означать возникновение проблемы. Контроль сопровождается графическим или цифровым отображением информации. Анализаторы могут накапливать и хранить информацию о состоянии сети с целью последующего его воспроизведения и анализа.

Сетевые тестеры. Это приборы, входящие в состав контрольно-измерительной аппаратуры, которая облегчает установку и техническое обслуживание локальных сетей. Тестеры линий передачи – хорошее средство проверки нового кабеля и отыскания неисправностей в

системе установленных кабелей. Они способны не только обнаруживать неисправность, но и сообщать сведения о ее характере и месте расположения.

12.3. Информационное обеспечение сети

Информационное обеспечение сети представляет собой единый информационный фонд, ориентированный на решаемые в сети задачи и содержащий базы данных общего применения, доступные для всех пользователей сети, базы данных индивидуального пользования, предназначенные для отдельных абонентов, базы знаний общего и индивидуального применения, автоматизированные базы данных – локальные и распределенные, общего и индивидуального назначения.

Для работы с сетевыми базами данных применяются обычные СУБД (системы управления локальными базами данных) и сетевые СУРБД (системы управления распределенными базами данных).

Информационное обеспечение (ИО) состоит из внешнего и внутреннего (рис. 12.19):

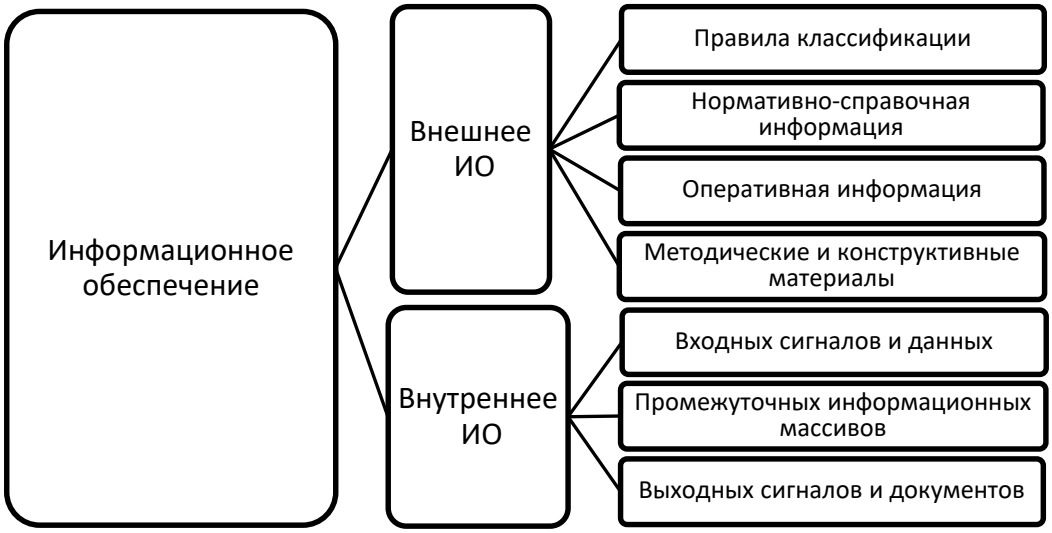


Рис. 12.19. Информационное обеспечение ИС

Внешнее ИО содержит правила классификации и кодирования, нормативно-справочную информацию, оперативную информацию, методические и инструктивные материалы.

Внутреннее ИО состоит из входных сигналов и данных, промежуточных информационных массивов, выходных сигналов и документов.

К информационному обеспечению предъявляются следующие общие требования:

- информационное обеспечение должно быть достаточным для поддержания всех автоматизируемых функций абонентов;
- для кодирования информации должны использоваться принятые у абонентов классификаторы;
- для кодирования входной и выходной информации, которая используется на высшем уровне управления, должны быть использованы классификаторы этого уровня;
- должна быть обеспечена совместимость с информационным обеспечением систем, взаимодействующих с разрабатываемой системой;
- формы документов должны отвечать требованиям корпоративных стандартов абонентов (или унифицированной системы документации);
- структура документов и экранных форм должна соответствовать характеристикам терминалов на рабочих местах конечных пользователей;
- графики формирования и содержание информационных сообщений, а также используемые аббревиатуры должны быть общеприняты в этой предметной области и согласованы с абонентами;
- в ИС должны быть предусмотрены средства контроля входной и результатной информации, обновления данных в информационных массивах, контроля целостности информационной базы, защиты от несанкционированного доступа.

Информационные ресурсы – это организованная совокупность документированной информации, включающая базы данных и знаний и другие массивы информации в информационных системах (библиотеки, архивы, делопроизводство и т.д.).

Перенесенные на электронные носители информационные ресурсы с помощью средств вычислительной техники и средств телекоммуникаций приобретают качественно новое состояние и становятся доступными для оперативного воспроизводства необходимой информации. Классификация информационных ресурсов по различным признакам приведена на рис. 12.20.

Рис. 12.20. Классификация информационных ресурсов

Основное звено ведения, наполнения и обеспечения доступа к информационным ресурсам – информационные системы. Информационные ресурсы являются базой для систем управления различного уровня.

12.4. Программное обеспечение сети

Программное обеспечение информационно-вычислительных сетей выполняет координацию работы основных звеньев и элементов сети; организует коллективный доступ ко всем ресурсам сети, динамическое распределение и перераспределение ресурсов с целью повышения эффективности обработки информации; выполняет техническое обслуживание и контроль работоспособности сетевых устройств. Сетевое программное обеспечение состоит из трех частей:

- общего программного обеспечения;
- системного программного обеспечения;
- специального программного обеспечения.

Общее программное обеспечение образуется из компонентов базового программного обеспечения отдельных компьютеров, входящих в состав сети, и включает в себя операционные системы, системы автоматизации программирования и системы технического обслуживания.

Системное программное обеспечение представляет собой комплекс программных средств, поддерживающих и координирующих взаимодействие всех ресурсов сети как единой системы.

Специальное программное обеспечение предназначено для максимального удовлетворения пользователей программами часто решаемых задач и соответственно содержит прикладные программы пользователя, ориентированные на специфику его предметной области.

Особая роль в программном обеспечении отводится операционным системам. Они имеются как в составе общего программного обеспечения (операционные системы отдельных компьютеров), так и в составе системного программного обеспечения.

Сетевая операционная система является *распределенной ОС* (РОС). Сложность ее однозначно определяется сложностью задач по управлению процессами в сети. РОС должна обеспечить управление сетью в любых допустимых для данной сети режимах. Для РОС характерен иерархический принцип построения. Многоуровневая организация РОС – стандарт любой ОС. В РОС принцип многоуровневости – принципиально необходим, и на других принципах построить такую систему невозможно. Для РОС существует единый стандарт *ISO/OSI* (*ISO – International Organization for Standardization, OSI – Open System Interconnection*). В нем зафиксировано семь уровней иерархии, и любая РОС должна отвечать этому стандарту, т.е. поддерживать все семь уровней.

В РОС входят управляющие программы, которые решают следующие задачи:

1. Удовлетворение запросов пользователей по использованию ресурсов сети.

2. Организация взаимодействия между различными прикладными программами: в сети в каждый момент времени могут исполняться различные типы программ. Часть из них не взаимодействует, а часть взаимодействует.

3. Синхронизация между прикладными программами при их одновременном обращении к одному и тому же ресурсу.

4. Удаленный ввод заданий, обмен файлами, передачу текстовых сообщений пользователям, защиту информации и ресурсов сети от несанкционированного доступа и т.д.

С помощью РОС планируется использование общесетевых ресурсов.

Различают три вида планирования:

Статическое планирование – для решения поступившей в систему к данному времени группы задач. Оно целесообразно, когда перечень задач стабилен и ограничен, для каждой задачи известны потребности в ресурсах сети и частота решения, а надобность в выполнении этих задач возникает неоднократно. Затраты на статическое планирование могут быть большими, зато сами планы – оптимальными в заданном смысле.

Динамическое планирование – производится в процессе функционирования сети непосредственно перед началом решения групп задач. С поступлением в систему каждой новой задачи составленный план обычно корректируется с учетом складывающейся ситуации по свободным и занятым ресурсам сети, наличию очередей задач и т.д. При этом используются методы получения приближенных планов, что объясняется недостатком информации о характеристиках решаемых задач.

Адаптивное планирование – непрерывно подстраивается план распределения ресурсов под характеристики прикладного процесса.

И, наконец, основной показатель эффективности организации вычислительного процесса в сети, планирования использования общесетевых ресурсов – время решения комплекса задач.

В большинство сетевых операционных систем встроена поддержка протоколов *TCP/IP, IPX/SPX, NetBEUT*.

Протоколы *TCP/IP* были разработаны в США для сети министерства обороны *ARPANet*. Ввиду высокой надежности управления сетью и универсальности в части используемых компьютеров (*IBM PC, Macintosh* и т. д.) и операционных систем (*Windows, UNIX* и т. д.) эти протоколы стали базовыми протоколами для сети *Internet*.

Протоколы *SPX/IPX* разработаны фирмой *Novell*. Отличительная особенность этих протоколов – маршрутизация, обеспечивающая кратчайший путь для передачи данных по сети и гарантированное установление надежной связи при этой передаче. Выбор кратчайшего пути основан на следующем механизме. Машина-источник посылает по сети широковещательный запрос по всем путям до машины-приемника. Путь, обеспечивший минимальную задержку в полу-

чении ответного эхо-сигнала, принимается за кратчайший. Этот механизм, конечно, существенно увеличивает трафик по сети и в этом его основной недостаток.

Протокол *NetBEUT* – детище фирмы *IBM* и создавался для обслуживания небольших сетей, в которых он очень популярен ввиду своей простоты и высокой скорости работы. Но в нем отсутствует маршрутизация и его поддерживают только операционные системы фирм *IBM* и *Microsoft* (не поддерживает, например, ОС *UNIX*).

Клиентское программное обеспечение. Для работы с сетью на клиентских рабочих станциях должно быть установлено клиентское программное обеспечение, которое предоставляет доступ к ресурсам, расположенным на сетевом сервере. Три наиболее важных компонента клиентского программного обеспечения – редиректоры (*redirector*), распределители (*designator*) и имена *UNC* (*UNC pathnames*).

Редиректоры

Редиректор – сетевое программное обеспечение, которое принимает запросы ввода/вывода для удаленных файлов, именованных каналов или почтовых слотов и затем переназначает их сетевым сервисам другого компьютера. Редиректор перехватывает все запросы, поступающие от приложений, и анализирует их.

Фактически существуют два типа редиректоров, используемых в сети:

1) клиентский редиректор (*client redirector*);

2) серверный редиректор (*server redirector*).

Оба редиректора функционируют на представительском уровне модели *OSI*. Когда клиент делает запрос к сетевому приложению или службе, редиректор перехватывает этот запрос и проверяет, является ли ресурс локальным (находящимся на запрашивающем компьютере) или удаленным (в сети). Если редиректор определяет, что это локальный запрос, он направляет запрос центральному процессору для немедленной обработки. Если запрос предназначен для сети, редиректор направляет запрос по сети к соответствующему серверу. По существу, редиректоры скрывают от пользователя сложность доступа к сети. После того как сетевой ресурс определен, пользователи могут получить к нему доступ без знания его точного расположения.

Распределители

Распределитель (*designator*) представляет собой часть программного обеспечения, управляющую присвоением букв накопителя (*drive letter*) как локальным, так и удаленным сетевым ресурсам или разделяемым дисководам, что помогает во взаимодействии с сетевыми ресурсами. Когда между сетевым ресурсом и буквой локального накопителя создана ассоциация, известная также как отображение дисковода (*mapping a drive*), распределитель отслеживает присвоение такой буквы дисковода сетевому ресурсу. Затем, когда пользователь или приложение получат доступ к диску, распределитель заменит букву дисковода на сетевой адрес ресурса, прежде чем запрос будет послан редиректору.

Имена UNC

Редиректор и распределитель являются не единственными методами, используемыми для доступа к сетевым ресурсам. Большинство современных сетевых операционных систем распознают имена *UNC* (*Universal Naming Convention* – Универсальное соглашение по наименованию). *UNC* представляют собой стандартный способ именования сетевых ресурсов. Эти имена имеют форму *\\Имя_сервера\имя_ресурса.* Способные работать с *UNC* приложения и утилиты командной строки используют имена *UNC* вместо отображения сетевых дисков.

Вопросы к компьютерному тестированию

1. Что понимают под линией связи, каналом связи, каналом передачи данных?
2. Перечислите виды линий связи в зависимости от физической среды передачи данных.
3. Какие линии связи используют в магистральных сетях, региональных и местных системах, локальных сетях?
4. Какой из оптоволоконных кабелей имеет лучшие оптические, потребительские характеристики?
5. Какие серверы выполняют функции обеспечения секретности данных, удаленную обработку заданий, защиты от проникновения извне?

6. В какой степени содержимое кэш *proxy*-сервера при выполнении функции кэширования доступно для пользователей?
7. Какие из компонентов компьютерной сети выполняют функции управления распределением сетевых ресурсов, организации обмена данными, объединения сегментов локальной сети с шиной, формирования сети?
8. Какой из компонентов компьютерной сети выполняет ряд «интеллектуальных» функций при управлении трафиком, функции согласования цифровых с аналоговыми сигналами, контроля качества функционирования сети, отыскания неисправностей в системе установленных кабелей?
9. Каково основное назначение брандмауэра в компьютерной сети?
10. Какие концентраторы используют в смешанных сетях с сегментами *Ethernet* и *Token Ring*?
11. Какие аппаратные средства, используемые в компьютерной сети, обеспечивают передачу данных между сегментами определенной длины?
12. Какими основными функциями обладает мост при объединении кабельных сегментов компьютерной сети?
13. Привести название уровня модели ВОС, на котором выполняют свои функции маршрутизаторы и шлюзы?
14. Какой из внутренних протоколов маршрутизаторов компьютерной сети принимает решения на основании таблицы маршрутизации, использует алгоритм, основанный на анализе состояния связи?
15. Какие устройства сетевого оборудования компьютерной сети осуществляют равномерное распределение потоков данных, протокольное преобразование для всех семи уровней модели ВОС, преобразование сообщения из одного формата в другой?
16. Какое устройство сетевого оборудования компьютерной сети повторяет каждый широковещательный пакет всем своим портам?
17. Какие устройства сетевого оборудования компьютерной сети отправляют пакет только тому порту, к которому подключено адресуемое устройство, осуществляют контроль качества функционирования сети?

18. Какую полосу частот использует модем для передачи данных по акустическому каналу, для приема данных по акустическому каналу, для передачи сигнала «1» по акустическому каналу, для передачи сигнала «0» по акустическому каналу методом *FSK*?
19. Какой сдвиг фазы сигнала использует модем при передаче сочетания бит 01, 10 методом *PSK*?
20. Назовите режимы передачи команд *PC* и ответов модема при работе в составе компьютерной сети.
21. В каком из режимов передачи команд *PC* и ответов модема передаваемая команда сопровождается старт- и стоп-битами?
22. Какие основные узлы включает абонентская, телекоммуникационная системы?
23. Какие задачи являются главными для вычислительных систем, для компьютерных сетей?
24. Что относят к основным средствам аппаратного, информационного обеспечения компьютерных сетей?
25. На какие группы подразделяют программное обеспечение компьютерных сетей?
26. К какой группе программного обеспечения относят программы для контроля работоспособности элементов, библиотеки стандартных программ, операционные системы?
27. На каких главных принципах строится распределенная операционная система?
28. Какой единый стандарт используется в распределенных операционных системах?
29. Какой вид планирования используют РОС при распределении общесетевых ресурсов до начала решения поступившей в систему к данному времени группы задач?
30. Какой вид планирования используют РОС при распределении общесетевых ресурсов в процессе функционирования сети непосредственно перед началом решения групп задач, при непрерывной подстройке ресурсов под характеристики прикладного процесса?

Глава 13

ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ. УПРАВЛЕНИЕ ДОСТУПОМ, СТАНДАРТЫ ПРОЕКТИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ

Рассматриваемые вопросы:

13.1. Определение и преимущества.
13.2. Классификация ЛВС.
13.3. Основные характеристики и области применения ЛВС.
13.4. Организация управления ЛВС.
13.5. Методы доступа к передающей среде в локальных вычислительных сетях.
13.6. Стандарты проектирования и использования сетей.

13.1. Основные определения и преимущества

Локальная вычислительная сеть – ЛВС (англ. *LAN – Lokal Area Network*) относится к географически ограниченным (территориально или производственно) аппаратно-программным реализациям, в которых несколько компьютерных систем связаны друг с другом с помощью соответствующих средств коммуникаций и работают под управлением сетевой операционной системы и сетевого программного обеспечения.

Компьютерные системы расположены, как правило, на сравнительно небольшом удалении друг от друга (до 10 км). Локальная сеть обычно предназначается для сбора, передачи, рассредоточенной и распределенной обработки информации в пределах одной лаборатории, отдела, офиса или фирмы, часто специализируется на выполнении определенных функций в соответствии с профилем деятельности фирмы и отдельных ее подразделений. Во многих случаях ЛВС, обслуживающая свою локальную информационную систему, связана с другими вычислительными сетями – внутренними или внешними, вплоть до региональных или глобальных сетей.

В ЛВС каждый ПК называется *рабочей станцией*, за исключением одного или нескольких компьютеров, которые предназначены для выполнения функций *файл-серверов.* Каждая рабочая станция и файл-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.

Преимущества, получаемые при сетевом объединении персональных компьютеров:

• *Разделение ресурсов* позволяет экономно использовать ресурсы, например, управлять периферийными устройствами, такими как лазерные печатающие устройства, со всех присоединенных рабочих станций.

• *Разделение данных* предоставляет возможность доступа и управления базами данных с периферийных рабочих мест, нуждающихся в информации.

• *Разделение программных средств* предоставляет возможность одновременного использования централизованных, ранее установленных программных средств.

• *При разделении ресурсов процессора* возможно использование вычислительных мощностей для обработки данных другими системами, входящими в сеть. Предоставляемая возможность заключается в том, что на имеющиеся ресурсы не «набрасываются» моментально, а только лишь через специальный процессор, доступный каждой рабочей станции.

• *Многопользовательский режим*. Многопользовательские свойства системы содействуют одновременному использованию централизованных прикладных программных средств, ранее установленных и управляемых, например, если пользователь системы работает с другим заданием, то текущая выполняемая работа отодвигается на задний план.

13.2. Классификация ЛВС

Для деления ЛКС на группы используются определенные классификационные признаки.

По назначению ЛВС их можно разделить на следующие группы:

• вычислительные, выполняющие преимущественно расчетные работы;

• информационно-вычислительные, кроме расчетных выполняющие работу по информационному обслуживанию пользователей;

• информационные, выполняющие в основном информационное обслуживание пользователей (создание и оформление документов, доставку пользователю директивной, текущей, справочной и другой нужной ему информации);

• информационно-поисковые – разновидность информационных сетей, специализирующихся на поиске информации в сетевых хранилищах по нужной пользователю тематике;

• информационно-советующие, обрабатывающие текущую организационную, техническую и технологическую информацию и вырабатывающие результирующую информацию для поддержки принятия пользователем правильных решений;

• информационно-управляющие, обрабатывающие текущую техническую и технологическую информацию и вырабатывающие результирующую информацию, на базе которой автоматически вырабатываются воздействия на управляемую систему, и т. д.

По топологии ЛВС делятся на шинные, петлевые, радиальные, полносвязные, иерархические и смешанные.

Существует параллельная классификация вычислительных сетей, в которой локальные сети определены несколько иначе: локальной сетью считается компьютерная сеть, обслуживающая нужды одного предприятия, одной корпорации. Среди таких вычислительных сетей выделяют:

• *Локальные сети рабочих групп*, обычно объединяют ряд ПК, работающих под управлением одной операционной среды. В ряду компьютеров часто выделяются специализированные серверы, предназначенные для выполнения функций файлового сервера, сервера печати, факс-сервера.

• *Локальные сети отделов* используются небольшой группой сотрудников предприятия, работающих в одном отделе (отдел кадров, бухгалтерия, отдел маркетинга и т. п.). В отделе может насчитываться до сотни компьютеров. Чаще всего такая сеть имеет несколько выделенных серверов, специализированных для таких ресурсов, как программы-приложения, базы данных, лазерные принтеры, модемы и т. д.

Такие сети, как правило, используют одну сетевую технологию и также одну (максимум две) операционную систему. Территориально они чаще всего расположены в одном здании.

• *Сети кампусов* получили название от слова *campus* – студенческий городок. Основное назначение этих сетей – объединение нескольких мелких сетей в одну. Сети кампусов могут занимать значительные территории и объединять много разнородных сетей. Основное назначение этих сетей – обеспечить взаимодействие между сетями отделов и рабочих групп и создать доступ к базам данных предприятия и другим дорогостоящим сетевым ресурсам. На уровне сети кампуса решаются многие проблемы интеграции неоднородного программного и технического обеспечения. Ресурсы глобальной сети *Internet* сети кампусов не используют.

• *Корпоративные сети* – сети масштаба всего предприятия, корпорации. Они могут охватывать большие территории, вплоть до работы на нескольких континентах. Ввиду высокой стоимости индивидуальных выделенных коммуникаций и плохой защищенности от несанкционированного доступа коммутируемых каналов связи они чаще всего используют коммуникационные возможности *Internet*, и поэтому территориальное размещение для таких сетей роли не играет. Корпоративные сети относят к особой разновидности локальных сетей, имеющих значительную территорию охвата. Ввиду быстрого развития и больших перспектив корпоративных сетей они рассмотрены в отдельном разделе.

По типам используемых компьютеров они делятся:

• на однородные;

• неоднородные.

В однородных ЛВС используются одинаковые типы компьютеров, имеющие одинаковые операционные системы и однотипный состав абонентских средств. В однородных сетях значительно проще выполнять многие распределенные информационные процедуры (в качестве классического примера можно назвать организацию и использование распределенных баз данных).

По количеству подключенных к сети компьютеров сети можно разделить на малые, объединяющие до 10 – 15 машин, средние – до 50 машин и большие – свыше 50 машин.

По территориальной расположенности ЛВС делятся на компактно размещенные (все компьютеры расположены в одном помещении) и распределенные (компьютеры сети размещены в разных помещениях).

По пропускной способности ЛВС делятся на три группы:

- ЛВС с малой пропускной способностью (скорости передачи данных в пределах до десятка мегабит в секунду), использующие чаще всего в качестве каналов связи тонкий коаксиальный кабель или витую пару;
- ЛВС со средней пропускной способностью (скорости передачи данных несколько десятков мегабит в секунду), использующие чаще всего в качестве каналов связи толстый коаксиальный кабель или экранированную витую пару;
- ЛВС с большой пропускной способностью (скорости передачи данных сотни и даже тысячи мегабит в секунду), использующие чаще всего в качестве каналов связи волоконно-оптические кабели.

По организации управления ЛВС делятся:

- на ЛВС с централизованным управлением (серверные сети);
- ЛВС с децентрализованным управлением (одноранговые сети).

В *сетях с централизованным управлением* (их называют двухранговыми, или серверными, сетями) выделяются одна или несколько машин (центральных систем или органов), управляющих работой сети.

Такие сети отличаются простотой обеспечения функций взаимодействия между АС ЛКС, более надежной системой защиты информации, но их применение целесообразно при сравнительно небольшом числе АС в сети.

Примеры сетевых операционных систем для таких сетей: *MS LAN Manager, IBM* и *Novell NetWare*.

Сети с децентрализованным (распределенным) управлением, или одноранговые (*peer-to-peer*), не имеют выделенных серверов, функции управления сетью передаются по очереди от одной РС к другой. Сетевая операционная система распределена по всем рабочим станциям (на каждом компьютере должны быть программные средства администрирования сетью).

Каждая станция сети может выполнять функции как клиента, так и сервера. Она может обслуживать запросы от других рабочих станций и направлять свои запросы на обслуживание в сеть.

Пользователю сети доступны все периферийные устройства, подключенные к другим станциям (магнитные и оптические диски, принтеры, сканеры, плоттеры и т. д.). Но отсутствие серверов в сети не позволяет администратору централизованно управлять ресурсами. Здесь облегчается совместная работа групп пользователей, но производительность сети понижается.

Недостатки одноранговых сетей: зависимость эффективности функционирования сети от количества АС, сложность управления сетью, сложность обеспечения защиты информации от несанкционированного доступа.

Одноранговые сети создаются на базе таких сетевых операционных систем, как *Artisoft LANtastic, Novell NetWare Lite*, оболочки *MS Windows for Workgroups.*

13.3. Основные характеристики и области применения ЛВС

К основным характеристикам ЛВС относятся следующие:

- территориальная протяженность сети (длина общего канала связи);
- максимальная скорость передачи данных;
- максимальное число АС в сети;
- максимально возможное расстояние между рабочими станциями в сети;
- топология сети;
- вид физической среды передачи данных;
- максимальное число каналов передачи данных;
- тип передачи сигналов (синхронный или асинхронный);
- метод доступа абонентов в сеть;
- структура программного обеспечения сети;
- возможность передачи речи и видеосигналов;
- условия надежной работы сети;
- возможность связи ЛКС между собой и сетью более высокого уровня;
- возможность использования процедуры установления приоритетов при одновременном подключении абонентов к общему каналу.

К числу наиболее типичных областей применения ЛКС относятся следующие:

• обработка текстов – это одна из наиболее распространенных функций средств обработки информации, используемых в ЛКС, которая обеспечивает реальный переход к «безбумажной» технологии;

• организация собственных информационных систем, содержащих автоматизированные базы данных – индивидуальные и общие, сосредоточенные и распределенные;

• обмен информацией между АС сети – важное средство сокращения до минимума бумажного документооборота;

• обеспечение распределенной обработки данных, связанное с объединением АРМ всех специалистов данной организации в сеть;

• поддержка принятия управленческих решений, предоставляющая руководителям и управленческому персоналу организации достоверную и оперативную информацию, необходимую для оценки ситуации и принятия правильных решений;

• организация электронной почты, позволяющей руководителям и всем сотрудникам предприятия оперативно получать необходимые сведения;

• коллективное использование дорогостоящих ресурсов, таких как высокоскоростные печатающие устройства, запоминающие устройства большой емкости, мощные средства обработки информации, прикладные программные системы, базы данных, базы знаний.

В зависимости от характера деятельности организации, в которой развернута одна или несколько локальных сетей, указанные функции реализуются в определенной комбинации. Кроме того, могут выполняться и другие функции, специфические для данной организации.

13.4. Организация управления ЛВС

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

Рассмотрим наиболее распространенные три вида архитектур:

1) Архитектура терминал-главный компьютер;

2) Одноранговая архитектура;

3) 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 (рис. 13.1).

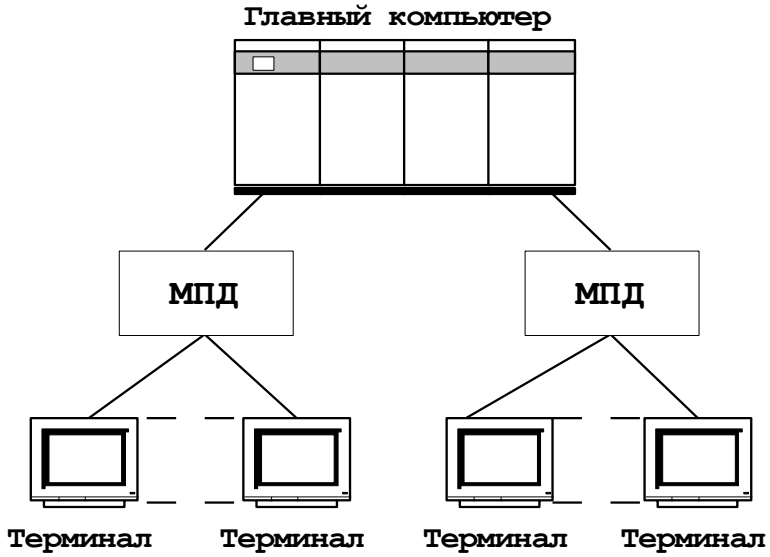


Рис. 13.1. Архитектура терминал-главный компьютер

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, как представлено на рис. 13.1, через мультиплексоры передачи данных (МПД) взаимодействует с терминалами.

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

Одноранговая сеть (peer-to-peer)

Это сеть без централизованного управления, когда нет единого центра управления взаимодействием рабочих станций и нет единого устройства для хранения данных. Функции управления сетью передаются от одной станции к другой. Сетевая операционная система распределена по всем рабочим станциям (на каждом компьютере должны быть программные средства администрирования сетью) (рис. 13.2).

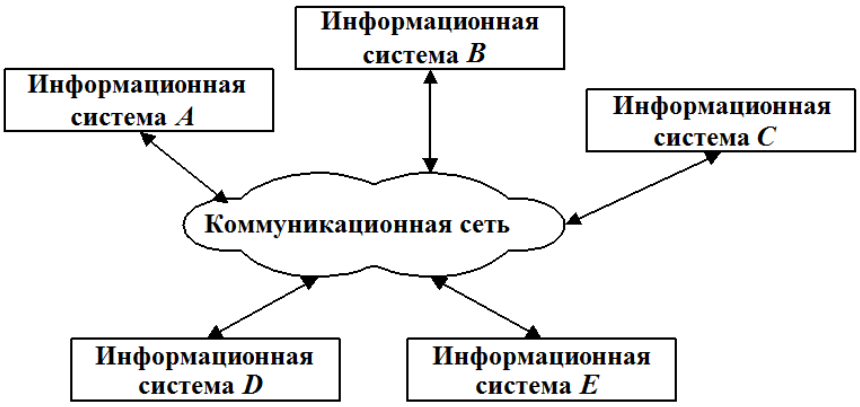


Рис. 13.2. Структура одноранговой сети

Каждая станция сети может выполнять функции как клиента, так и сервера. Она обслуживает запросы от других рабочих станций и направляет свои запросы на обслуживание в сеть. Пользователю сети доступны все периферийные устройства, подключенные к другим станциям.

Отсутствие серверов в сети не позволяет администратору централизованно управлять ресурсами. Каждый компьютер, включенный в одноранговую сеть, имеет свои собственные сетевые программные средства, а необходимость прямого взаимодействия компьютеров друг с другом по мере расширения системы приводит к слишком большому количеству связей между рабочими станциями. Эффективно управлять такой системой практически невозможно.

Достоинства одноранговых сетей:

- низкая стоимость;
- нет необходимости в администраторе;
- высокая надежность.

Недостатки:

- возможность подключения небольшого числа рабочих станций (не более 10);
- сложность управления сетью;
- трудности обновления и изменения программного обеспечения станций;
- сложность обеспечения защиты информации.

Одноранговые сети создаются на базе таких сетевых операционных систем, как *Artisoft LANtastic, Novell NetWare Lite*, оболочки *MS Windows for Workgroups.*

Серверные локальные сети

Один из компьютеров (сервер) реализует процедуры, предназначенные для использования всеми рабочими станциями, управляет взаимодействием рабочих станций и выполняет целый ряд сервисных функций.

Сервер выполняет запрос, поступивший от клиента. Результаты выполнения запроса передаются клиенту. Сервер обеспечивает хранение данных общего использования, организует доступ к этим данным и передает данные клиенту (рис. 13.3).

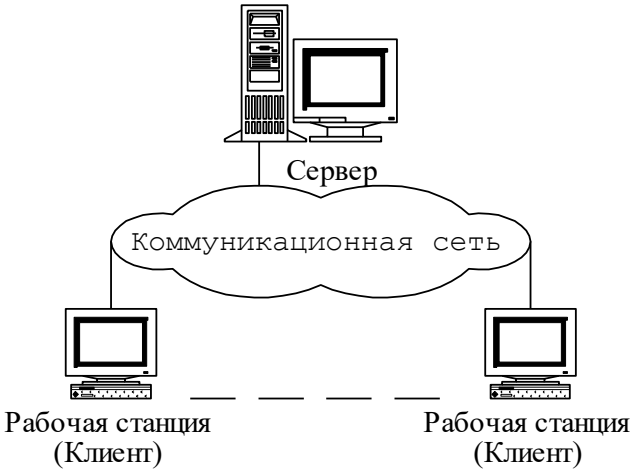


Рис. 13.3. Структура серверной сети

Процесс, который вызывает сервисную функцию с помощью определенных операций, называется *клиентом*. Им может быть программа или пользователь. На рис. 13.4 приведен перечень сервисов в архитектуре клиент-сервер.

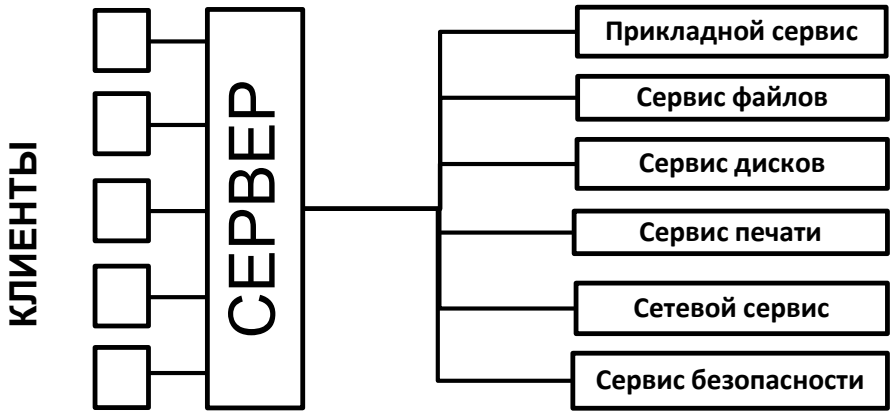


Рис. 13.4. Перечень сервисов в архитектуре клиент-сервер

Клиенту непосредственно доступны ресурсы сети, имеющиеся только на сервере (серверах при нескольких специализированных серверах). Данные и программы, хранящиеся на дисках чужих рабочих станций, могут быть доступны пользователю только через сервер или с помощью установленной в сети специальной программы доступа к ресурсам рабочих станций.

Системы, в которых сервер выполняет только процедуры организации, хранения и выдачи клиентам нужной информации, называются системами «файл-сервер», или сетями с выделенным сервером; те же системы, в которых на сервере наряду с хранением выполняется и содержательная обработка информации, принято называть системами «клиент-сервер».

В системе «клиент-сервер» сервер играет активную роль: он не просто выдает на запрос весь файл, а может предварительно обработать информацию и выдать клиенту результаты решения задачи или отобрать именно те записи файла, которые и интересуют клиента в удобном для клиента представлении. Такая технология, кроме всего прочего, способствует и меньшей загрузке каналов связи сети.

Клиент-серверные системы иногда подразделяют также на две группы:

- системы, в которых клиент, решая свои задачи на сервере, использует свое прикладное программное обеспечение (такие системы часто называют системами с *толстым клиентом*);
- системы, в которых клиент, решая свои задачи на сервере, использует прикладное программное обеспечение, размещенное на сервере (такие системы часто называют системами с *тонким клиентом*); типичным примером данных систем являются ЛВС, использующие в качестве рабочих станций сетевые компьютеры.

Сервер, работающий по технологии «файл-сервер», сам называется файл-сервером; работающий по технологии «клиент-сервер» – сервером приложений.

Достоинства серверных локальных вычислительных сетей:

- отсутствие ограничений на число рабочих станций;
- простота управления по сравнению с одноранговыми сетями;
- высокое быстродействие;
- надежная система защиты информации.

Недостатки:

- высокая стоимость из-за выделения одного или нескольких компьютеров под сервер;
- зависимость быстродействия и надежности сети от сервера;
- меньшая гибкость по сравнению с одноранговой сетью.

Серверные сети весьма распространенные; примеры сетевых операционных систем для таких сетей: *MS LAN Manager, Windows NT* фирмы *Microsoft; UNIX* фирмы *AT&T; Linux* и *Novell NetWare.*

Выбор архитектуры сети

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

Следует выбрать одноранговую сеть, если:

- количество пользователей не превышает десяти;
- все машины находятся близко друг от друга;
- скромные 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;
- требуются централизованное управление, безопасность, управление ресурсами или резервное копирование;
- необходим специализированный сервер;
- нужен доступ к глобальной сети;
- требуется разделять ресурсы на уровне пользователей.

13.5. Методы доступа к передающей среде в локальных вычислительных сетях

Доступ к передающей среде – это прежде всего «захват передающей среды». Сам «захват» включает несколько составляющих:

1) определение, какая следующая рабочая станция может использовать передающую среду;

2) набор правил, используемых сетевым оборудованием для того, чтобы направлять поток данных через сеть;

3) набор признаков, по которым делят сетевое оборудование на классы.

В ЛВС, использующих для передачи информации моноканал (т.е. канал связи, одновременно используемый несколькими абонентами), важным является вопрос доступа клиентов к этому каналу. Чтобы сделать доступ эффективным, необходимы специальные механизмы – *методы доступа.* Методы доступа обеспечиваются соответствующими протоколами.

Протокол управляет форматами сообщений, временными интервалами, последовательностью передачи и контролем достоверности передачи, а также обеспечением достоверности передачи.

Для организации эффективного доступа к моноканалу используются принципы частотной или временной модуляции. Наибольшее применение в простых сетях получили принципы временной модуляции, то есть временного разделения сообщений, передаваемых по моноканалу. Существует несколько групп методов доступа, основанных на временном разделении:

- централизованные и децентрализованные;
- детерминированные и случайные.

Централизованный доступ управляется из центра управления сетью, например от сервера. *Децентрализованные методы доступа* функционируют на основе протоколов, принятых к исполнению всеми рабочими станциями сети без каких-либо управляющих воздействий со стороны центра.

Детерминированный доступ обеспечивает наиболее полное использование моноканала и описывается протоколами, дающими гарантию каждой рабочей станции на определенное время доступа к моноканалу. При *случайном доступе* обращения станций к моноканалу могут выполняться в любое время, но нет гарантий, что каждое такое обращение позволит реализовать эффективную передачу данных.

При централизованном доступе каждый клиент может получать доступ к моноканалу:

- по заранее составленному расписанию – статическое разделение времени канала;
- по жесткой временной коммутации через определенные промежутки времени (например, через каждые 0,5 с), задаваемые электронным коммутатором – динамическое детерминированное разделение времени канала;

• по гибкой временной коммутации путем опроса рабочих станций на предмет выяснения необходимости доступа;

• при получении полномочий в виде специального пакета – маркера.

Первые два метода не обеспечивают эффективную загрузку канала, ибо при предоставлении доступа некоторые клиенты могут быть не готовы к передаче данных, и канал в течение выделенного им отрезка времени будет простаивать.

К децентрализованным детерминированным методам относятся:

• метод передачи маркера;

• метод включения маркера.

Оба метода используются преимущественно в сетях с петлевой (кольцевой) топологией и основаны на передаче по сети специальных пакетов – маркеров, сегментов.

Маркер – служебный пакет определенного формата, в который клиенты сети могут помещать свои информационные пакеты. Последовательность передачи маркера по сети от одной рабочей станции к другой задается сервером (управляющей станцией). Рабочая станция, имеющая данные для передачи, анализирует, свободен ли маркер. Если маркер свободен, станция помещает в него пакет/пакеты своих данных, устанавливает в нем признак занятости и передает маркер дальше по сети. Станция, которой было адресовано сообщение (в пакете обязательно есть адресная часть), принимает его, сбрасывает признак занятости и отправляет маркер дальше. Данный метод доступа для сетей с шинной и радиальной топологиями обеспечивается распространенным протоколом *Arcnet* корпорации *Datapoint*.

Метод передачи маркера во многом подобен методу передачи полномочий, но движением маркера из центра сети не управляют. Такой метод доступа реализуется в сетях с кольцевой и радиальной топологией широко известным протоколом *Token Ring*, разработанным фирмой *IBM*, и протоколом *FDDI* института *ANSI*.

Метод включения маркера также использует свободно циркулирующий по сети маркер. Рабочая станция, получившая маркер, может передать свои данные, даже если пришедший маркер занят. В последнем случае станция приостанавливает движение поступившего маркера (временно запоминает его в буферной памяти) и вместо него формирует новый маркер с включенным в него своим пакетом данных.

Дальше по сети станция сначала посылает свой новый маркер, а затем уже ранее поступивший «чужой» маркер.

Случайные методы доступа основаны на равноправности всех станций сети и их возможности в любой момент времени обратиться к моноканалу с целью передачи данных. Поскольку возможны одновременные попытки передачи данных со стороны нескольких станций, между ними часто возникают *коллизии* (конфликты, столкновения), в связи с чем случайный метод доступа часто называют «методом состязаний».

Сокращение числа конфликтных ситуаций обеспечивается путем предварительного прослушивания моноканала для выявления его занятости станцией, желающей передать данные. Если канал занят, станция возобновляет свою попытку передачи данных через небольшой интервал времени. Если все же передачу данных начнут одновременно две станции, то возникает коллизия и данные в моноканале искажаются. Обе конфликтующие станции будут вынуждены передать свои данные повторно.

Метод состязаний может быть рекомендован для использования в сетях с небольшим количеством абонентов, моноканал которых загружен мало (метод не может обеспечить хорошую загрузку канала из-за часто возникающих конфликтных ситуаций). Этот метод для сетей с шинной топологией реализуется чрезвычайно популярным протоколом *Ethernet* фирмы *Xerox*.

13.6. Стандарты проектирования и использования сетей

В 1980 г. в Международном институте инженеров по электротехнике и радиоэлектронике (*Institute of Electronics Engineers – IEEE*) был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов *IEEE* 802-*x*, которые содержат рекомендации по проектированию нижних уровней локальных сетей. Позже результаты работы этого комитета легли в основу комплекса международных стандартов *ISO* 8802-1...5. Эти стандарты были созданы на основе очень распространенных фирменных стандартов сетей *Ethernet, Arcnet и Token Ring*.

Помимо *IEEE* в работе по стандартизации протоколов локальных сетей принимали участие и другие организации. Так, для сетей, работающих на оптоволокне, американским институтом по стандартизации *ANSI* был разработан стандарт *FDDI*, обеспечивающий скорость передачи данных 100 Мб/с. Работы по стандартизации протоколов ведутся также ассоциацией *ECMA*, которой приняты стандарты *ECMA*-80, 81, 82 для локальной сети типа *Ethernet* и впоследствии стандарты *ECMA*-89,90 по методу передачи маркера.

Стандарты семейства *IEEE* 802.*x* охватывают только два нижних уровня семиуровневой модели *OSI* – физический и канальный. Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику локальных сетей. Старшие же уровни, начиная с сетевого, в значительной степени имеют общие черты как для локальных, так и для глобальных сетей.

Специфика локальных сетей также нашла свое отражение в разделении канального уровня на два подуровня, которые часто называют также уровнями. Канальный уровень (*Data Link Layer*) делится в локальных сетях на два подуровня:

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

Уровень LLC отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем.

Уровень MAC обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. В современных локальных сетях получили распространение несколько протоколов уровня *MAC*, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий, как *Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, l00VG-AnyLAN*.

Протоколы уровней *MAC* и *LLC* взаимно независимы – каждый протокол уровня *MAC* может применяться с любым протоколом уровня *LLC*, и наоборот.

Стандарты *IEEE* 802 имеют достаточно четкую структуру, приведенную на рис. 13.5.

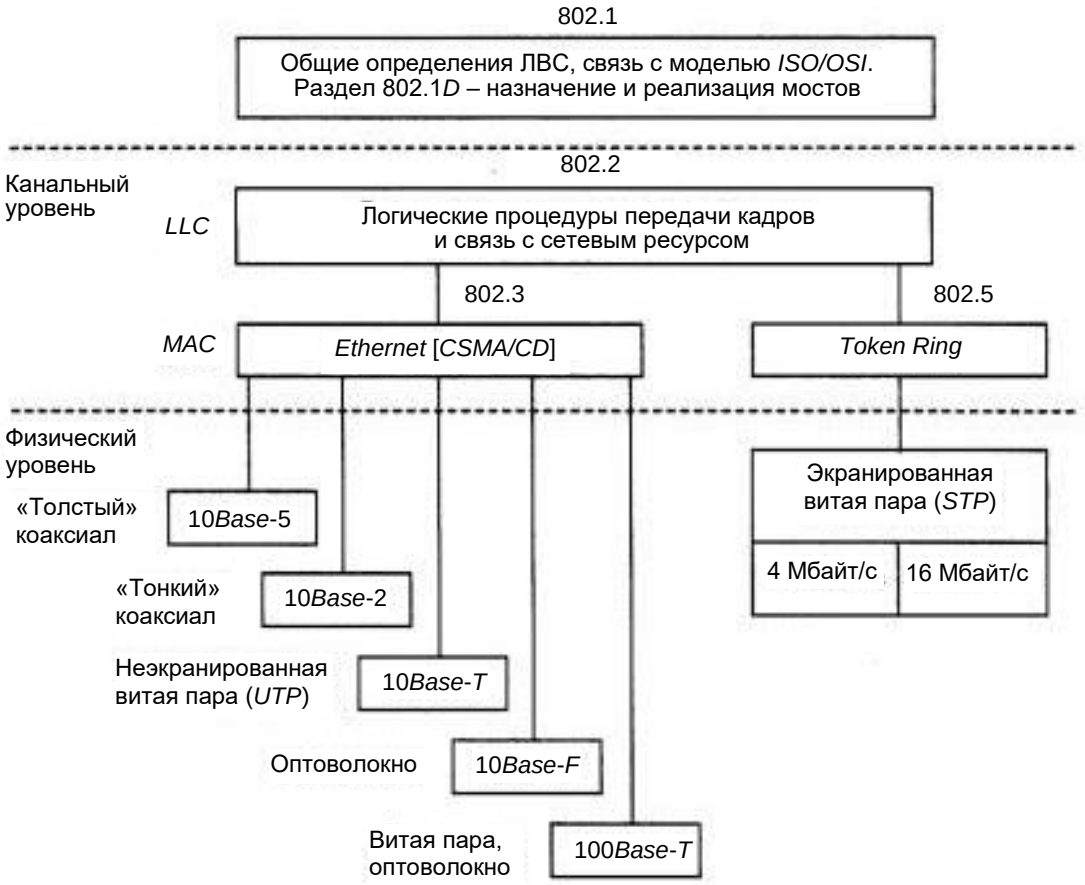


Рис. 13.5. Структура стандартов *IEEE* 802.*x*

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

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.

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.

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* (10*BaseT*, 10*Base*2, 10*Base*5).

Метод доступа *CSMA/CD*. 802.3 также включает технологии *Fast Ethernet* (100*BaseTx*, 100*BaseFx*, 100*BaseT*4).

100*BaseTx* – двухпарная витая пара. Используется метод *MLT*-3 для передачи сигналов 5-битовых порций кода 4*B*/5*B* по витой паре, а также имеется функция автопереговоров (*Auto-negotiation*) для выбора режима работы порта.

100*BaseT*4 – четырехпарная витая пара. Вместо кодирования 4*B*/5*B* в этом методе используется кодирование 8*B*/6*T*.

100*BaseFx* – многомодовое оптоволокно. Эта спецификация определяет работу протокола *Fast Ethernet* по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе хорошо проверенной схемы кодирования и передачи оптических сигналов, использующейся уже на протяжении ряда лет в стандарте *FDDI*. Как и в стандарте *FDDI*, каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника (*Rx*) и передатчика (*Tx*).

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*. Говорят, что 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.

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 Мб/с. Этот метод предусматривает следующие правила: все устройства, подключённые 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 трёх служебных старт/стоповых битов и восьми битов данных.

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*.

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

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

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.

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.

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

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

Стандарт 802.12 описывает рекомендации по использованию сетей 100*VG – AnyLAN* со скоростью100 Мб/с и методом доступа по очереди запросов и по приоритету (*Demand Priority Queuing – DPQ, Demand Priority Access – DPA*).

Технология 100*VG* – это комбинация *Ethernet и TokenRing* со скоростью передачи 100 Мб/с, работающая на неэкранированных витых парах. В проекте 100*Base-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. Имеются два уровня приоритетов – высокий и низкий.

Вопросы к компьютерному тестированию

1. Как называют абонентский компьютер ЛВС?
2. Как называют адаптер ЛВС, с помощью которого абонентские системы соединяются между собой?
3. Что является основным преимуществом, получаемым при сетевом объединении персональных компьютеров?
4. Как обычно называют группу ЛВС, обрабатывающую текущую техническую и технологическую информацию, при классификации по назначению?
5. Как обычно называют группу ЛВС, обеспечивающую взаимодействие между сетями отделов и рабочих групп и создающую доступ к базам данных предприятия и другим дорогостоящим сетевым ресурсам, при классификации по топологии?
6. Как обычно называют группу ЛВС, использующую одинаковые типы компьютеров, имеющую одинаковые операционные системы и однотипный состав абонентских средств, при классификации по типам используемых компьютеров?
7. Как обычно называют группу ЛВС, в которой клиенту непосредственно доступны ресурсы сети, имеющиеся только на сервере, при классификации по организации управления?
8. Как называют системы, в которых сервер выполняет только процедуры организации, хранения и выдачи клиентам нужной информации?
9. Как называют системы, в которых сервер выполняет активную роль, а именно обрабатывает информацию и выдает результаты решения задачи?
10. Какое название носят системы, в которых клиент, решая свои задачи на сервере, использует свое прикладное программное обеспечение?
11. Какое название носят системы, в которых клиент, решая свои задачи на сервере, использует прикладное программное обеспечение, размещенное на сервере?
12. Как обычно называют группу ЛВС, в которой сети не имеют выделенных серверов, функции управления сетью передаются по очереди от одной РС к другой, при классификации по организации управления?
13. Назовите наиболее распространенные три вида архитектур.
14. В какой из архитектур ЛВС вся обработка данных осуществляется одним или группой хост-компьютеров?

15. В какой из архитектур ЛВС функции управления сетью передаются от одной станции к другой?
16. В какой из архитектур ЛВС один из компьютеров реализует процедуры, предназначенные для использования всеми рабочими станциями?
17. Назовите основные методы доступа к передающей среде, используемые в ЛКС.
18. При каком методе доступа каждой рабочей станции передача разрешается только в определенные моменты времени?
19. При каком методе доступа приводится проверка на наличие свободного пространства и запрет на попытки прерывания?
20. При каком методе доступа каждая станция для передачи получает свой интервал времени (временной слот)?
21. При каком методе доступа рабочая станция записывает кадр для временного хранения в буфер и по мере передачи данных забирает оттуда?
22. При каком методе доступа рабочая станция использует маркер «свободен/занят»?
23. Приведите аббревиатуру части протокола *Ethernet*, которая определяет, когда следует посылать сообщение.
24. Приведите аббревиатуру части протокола, которая служит для разрешения ситуаций одновременной передачи сообщений.
25. Приведите название версии *Ethernet*, имеющей пропускную способность 100 Мб/с.
26. Приведите название версии *Ethernet*, имеющей пропускную способность 1000 Мб/с.
27. К каким группам методов относится метод доступа к локальной сети *Token Ring*?
28. Запишите число, в котором каждая последующая цифра означает номер поля из приведенного списка полей пакета по стандарту *IEEE* 802.3 технологии *Ethernet*. (*Контрольная сумма, назначение, признак начала, преамбула, набивка, длина, источник, данные*).
29. Как называют метод передачи пакетов протоколов верхнего (среднего) уровня, когда пакеты передаются и адресуются без подтверждения получения?
30. Как называют метод передачи пакетов протоколов верхнего (среднего) уровня, когда доставка сообщений подтверждается?

Глава 14

СТЕКИ ПРОТОКОЛОВ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ ЛВС

Рассматриваемые вопросы:

14.1. Стеки протоколов верхнего и среднего уровней.
14.1.1. Сетевые протоколы.
14.1.2. Транспортные протоколы.
14.1.3. Прикладные протоколы.
14.1.4. Стек *OSI* для протоколов верхнего и среднего уровней.
14.1.5. Архитектура стека протоколов *Microsoft TCP/IP*.
14.1.6. Адресация в *IP*-сетях.
14.1.7. Протоколы сопоставления адреса *ARP* и *RARP*.
14.1.8. Протокол *ICMP*.
14.1.9. Протокол *IGMP*.
14.1.10. Протокол *NDIS*.
14.1.11. Уровень сетевого интерфейса.
14.2. Настройка *IP*-адресации и маршрутизации.
14.2.1. Основы *IP*-адресации.
14.2.2. Классовая и бесклассовая *IP*-адресация.
14.2.3. IP-адреса для локальных сетей.
14.2.4. Основы IP-маршрутизации.
14.2.5. Назначение IP-адресов и проверка работоспособности *TCP/IP*.
14.3. Протоколы передачи данных нижнего уровня.
14.4. Определение основных характеристик системы передачи данных.

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. Это и стеки, являющиеся международными и национальными стандартами, и фирменные стеки, получившие распространение благодаря распространенности оборудования той или иной фирмы.

14.1. Стеки протоколов верхнего и среднего уровней

Протоколы верхнего и среднего уровней служат для обмена данными. Они предоставляют программам интерфейс для передачи данных методом дейтаграмм, когда пакеты адресуются и передаются без подтверждения получения, и методом сеансов связи, когда устанавливается логическая связь между взаимодействующими станциями (источником и адресатом) и доставка сообщений подтверждается.

Из протоколов этого уровня наиболее широкое применение в локальных сетях нашли протокол *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. Стек *IPX/SPX* – это сетевой протокол *NetWare*, причем *IPX* (*Internetwork Packet Exchange*) – протокол межсетевого обмена пакетами (дейтаграммами), а *SPX* (*Sequenced Packet Exchange*) – протокол последовательного обмена пакетами в сеансах связи.

Стеки протоколов верхнего и среднего уровней разбиваются на три группы:

- сетевые;
- транспортные;
- прикладные.

14.1.1. 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). Это 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*.

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*.

Система протоколов *Novel NetWare*, используемых для маршрутизации и направления пакетов.

14.1.2. Транспортные протоколы

Транспортные протоколы предоставляют следующие 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* используется для обеспечения доставки данных.

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

14.1.3. 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.

14.1.4. Стек OSI для протоколов верхнего и среднего уровней

Следует различать стек протоколов *OSI* и модель *OSI*. Стек *OSI* – это набор вполне конкретных спецификаций протоколов, образующих согласованный стек протоколов. 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 *сетевом* уровне реализованы протоколы как без установления соединений, так и с установлением соединений.

Транспортный протокол стека *OSI* скрывает различия между сетевыми сервисами с установлением и без установления соединения, так что пользователи получают нужное качество обслуживания независимо от нижележащего сетевого уровня. Для обеспечения этого 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.

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.

14.1.5. Архитектура стека протоколов Microsoft TCP/IP

Набор многоуровневых протоколов, или как называют стек *TCP/IP*, предназначен для использования в различных вариантах сетевого окружения.

Основные преимущества стека *TCP/IP* перед другими (например, перед стеком *IPX/SPX*):

- более удобная система *сетевой адресации;*
- возможность *фрагментации пакетов;*
- небольшое количество широковещательных сообщений.

Эти преимущества оказались решающими не только при построении глобальных сетей, объединяющих сети с разнородными архитектурами, но и при создании крупных корпоративных сетей.

В результате сегодня стек *TCP/IP* практически вытеснил все остальные – он используется и в небольших домашних сетях, и в глобальной сети *Internet*.

Поскольку стек *TCP/IP – общедоступный*, его стандарты (а также просто информационные материалы) публикуются в сети *Internet* в виде специальных документов под названием *RFC* (*Request for Comments* – запрос комментариев) с последовательно возрастающим номером. К примеру, спецификация протокола *IP* опубликована в *RFC 791*, а протокола *HTTP* версии 1.1 – в *RFC 2616*. Первый документ *RFC* был представлен еще в апреле 1969 г., а сейчас текущие номера *RFC* исчисляются десятками тысяч.

Для верхних и средних уровней модели *OSI* стек *TCP/IP* показан на рис. 14.1.

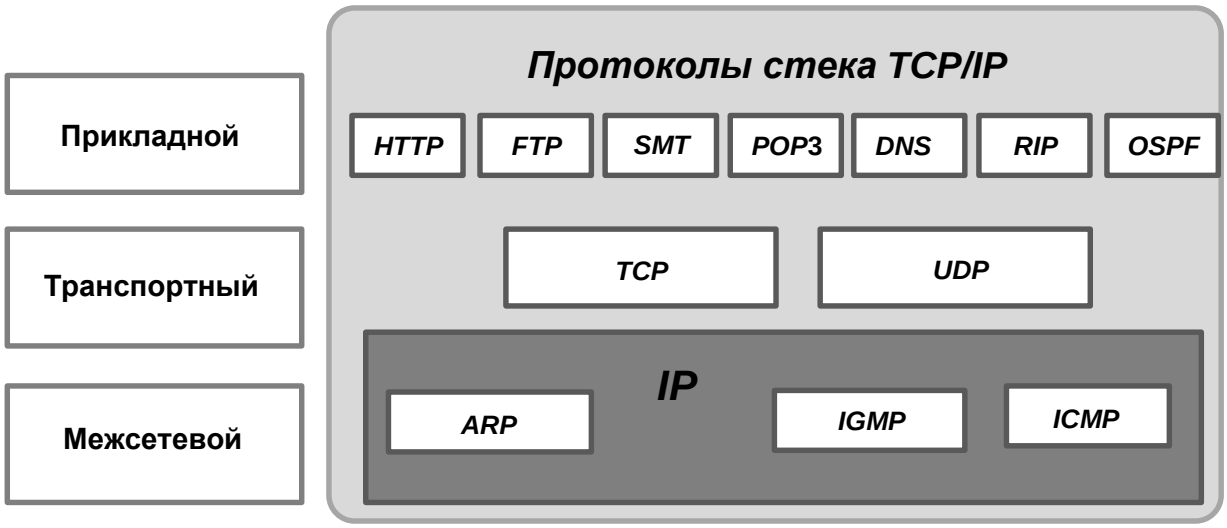


Рис. 14.1. Основные протоколы стека *TCP/IP* для верхних и средних уровней модели *OSI*

1. *На **сетевом уровне*** располагаются несколько протоколов:

- *протокол ARP* (*Address Resolution Protocol*), который является звеном, связывающим сетевой уровень с физическим. Он отвечает за преобразование сетевых *IP*-адресов в аппаратные *MAC*-адреса;
- *протокол RARP* (*Reverse Address Resolution Protocol*) осуществляет обратное преобразование *MAC*-адресов в *IP*-адреса (в операционных системах *Windows* поддержка протокола *RARP* не предусмотрена);
- *протокол ICMP* (*Internet Control Message Protocol*) предназначен для передачи сообщений об ошибках, диагностики доступности сетевого узла и маршрута доставки пакетов (именно его используют такие популярные утилиты, как *PING* и *TRACERT*);
- *протокол IGMP* (*Internet Group Management Protocol*) предназначен для управления группами компьютеров, например, при передаче в сетях потокового видео и звука, когда для снижения нагрузки на сеть пакет посылается по специальному адресу сразу нескольким компьютерам (многоадресная рассылка);
- *протокол IP* (*Internet Protocol*) – один из самых важных в стеке *TCP/IP*. Как следует из его названия («*IP*» переводится как «межсетевой протокол»), он отвечает за доставку *IP-дейтаграмм* (так правильно называются пакеты на уровне протокола *IP*), обеспечивая передачу пакета из одной сети в другую. О том, как это происходит, будет подробно изложено далее.

2. *На **транспортном уровне*** работают два протокола:

- *протокол TCP* (*Transmission Control Protocol – протокол управления передачей*) – основной протокол транспортного уровня. Обеспечивает установку соединения между отправителем и получателем, разбиение крупного блока информации (например, файла) на небольшие *TCP*-пакеты и их гарантированную доставку получателю (в нужном порядке и без ошибок). Соответственно протокол *TCP* применяется в тех приложениях, где важно обеспечить целостность при передаче данных;
- *протокол UDP* (*User Datagram Protocol*) в отличие от *TCP* не устанавливает соединения перед передачей информации и не обеспечивает надежной доставки данных, работая при этом

быстрее, чем *TCP*. Его используют там, где обеспечение доставки информации не особенно важно по сравнению со скоростью передачи (контроль за целостностью данных в этом случае возлагается на протокол *UDP*).

Представить себе работу протоколов *TCP* и *UDP* удобно путем аналогии с почтой. Если необходимо переслать объемный документ, а в письмо разрешается вкладывать не больше нескольких страниц текста, то в такой ситуации вначале хорошо бы договориться с получателем о системах обозначения в отправлении и о нумерации сообщений. Для этого нужно послать дополнительное письмо, извещающее получателя о намерении переслать объемный документ, в котором указать исходящий номер следующего сообщения.

В ответном письме получатель сообщает свои исходящие и входящие номера, а отправитель подтверждает получение этих номеров.

Таким образом, обе стороны согласуют номера сообщений, которые они позже будут ожидать друг от друга, что и означает установку связи.

Дальше остается только разделить документ большого объема на небольшие части и посылать каждую в отдельном письме, а получателю – подтверждать получение этих частей. Ошибки работы почты (если какое-то сообщение не дойдет до получателя из-за потери или повреждения письма либо придет вне очереди) легко определить по входящим и исходящим номерам, чтобы принять соответствующие меры – заново переслать утерянную часть или собрать страницы отправления в нужном порядке.

Примерно так же работает и протокол *TCP*:

- устанавливает соединение между компьютерами по определенным портам;
- на компьютере-отправителе разбивает информацию на пакеты, нумерует их и с помощью протокола *IP* передает получателю;
- на компьютере-получателе проверяет, все ли пакеты получены, а если пакет пропущен или поврежден, запрашивает у отправителя повторную пересылку;
- после получения всех пакетов закрывает соединение, собирает пакеты в нужном порядке и передает полученные данные приложению более высокого уровня.

Протокол же *UDP* в этой аналогии можно сравнить с рассылкой рекламных сообщений.

Никакого установления связи и подтверждения получения корреспонденции здесь нет – письма с рекламной информацией просто бросают в ваш почтовый ящик.

При этом ни отправителя, ни получателя надежность доставки информации или ее целостность, вообще говоря, не особенно беспокоят.

Очевидно, почтовые отправления в обоих этих примерах являются аналогами *IP*-пакетов, а почтальоны выполняют функции протокола *IP*.

Порт в *TCP* или *UDP* – это логический канал с определенным номером (от 0 до 65536), обеспечивающий текущее взаимодействие между отправителем и получателем. Порты позволяют компьютеру с одним *IP*-адресом параллельно обмениваться данными с множеством других компьютеров. Некоторые номера портов (так называемые «хорошо известные», или «*well-known*», порты с номерами от 0 до 1024) привязаны к определенным службам и приложениям, что позволяет клиентам легко обращаться к нужным им сетевым сервисам.

3. Наконец, самый богатый по набору протоколов – ***прикладной уровень*** стека *TCP/IP*.

Ниже в табл. 14.1 приведены самые популярные протоколы, а также зарезервированные для них порты. Заметим, что, хотя для протоколов обычно резервируются одинаковые номера портов и для *TCP*, и для *UDP*, в таблице приведены порты для наиболее часто применяемого протокола транспортного уровня (*TCP* или *UDP*).

Табл. 14.1. Протоколы стека *TCP/IP*

Протокол	**Назначение**	**Номер порта**
NTP (Network Time Protocol)	Протокол сетевого времени, используется для синхронизации системных часов компьютеров в сетях	123 (*UDP*)
DNS (Domain Name System, или Service)	Служба доменных имен; используется для преобразования (разрешения) понятных людям имен компьютеров (например, имен типа *WWW.microsoft.com*) в *IP*-адреса	53 (*TCP* и *UDP*)

Продолжение табл. 14.1

Протокол	**Назначение**	**Номер порта**
NetBIOS name service и WINS (Windows Internet Naming Service)	Служба имен *NetBIOS* и служба межсетевых имен *Windows*; используются для преобразования *NetBIOS*-имен компьютеров (например, имен типа *SERVER*) в *IP*-адреса	137 и 138 (*UDP*)
NetBIOS session service	Служба сеансов *NetBIOS*; используется для установления сеансов между компьютерами	139 (*TCP*)
LDAP (Light-weight Directory Access Protocol)	Простой протокол доступа к каталогу; используется для работы с различными сетевыми каталогами (например, со службой *Active Directory* в доменах на основе *Windows Server* 2003)	389 (*TCP*)
RPC (Remote Procedure Call)	Вызов удаленной процедуры; используется для работы со многими сетевыми службами в сетях Майкрософт	135 (*TCP*)
Telnet	Протокол для обеспечения терминального доступа к удаленным компьютерам	23 (*TCP*)
FTP (File Transfer Protocol)	Протокол передачи файлов, один из «старейших» протоколов *Internet*; используется для эффективной и надежной передачи файлов между клиентом и сервером *FTP*	20 и 21 (*TCP*)
TFTP (Trivial File Transfer Protocol)	Упрощенный вариант *FTP* (не имеет функций проверки пользователя при входе, просмотре каталогов и файлов сервера; используется только для записи/чтения файлов)	69 (*UDP*)
Gopher («суслик»)	Протокол *Gopher*; используется для доступа к текстовым информационным ресурсам на удаленном сервере	70 (*TCP*)
HTTP (HyperText Transfer Protocol)	Протокол передачи гипертекста, самый популярный сегодня протокол, используемый во Всемирной паутине (*World Wide Web*); описывает, каким способом нужно представлять данные (текстовые, аудио-, видео- и т. д.) на веб-серверах, как к ним обращаться с помощью веб-браузера (например, программы *Internet Explorer*) и как передавать эти данные	80 (*TCP*)
NNTP (Network News Transfer Protocol)	Протокол передачи сетевых новостей; используется для обмена сообщениями в системах телеконференций	119 (*TCP*)

Окончание табл. 14.1

Протокол	Назначение	Номер порта
SMTP (Simple Mail Transfer Protocol)	Простой протокол передачи почты; используется почтовыми серверами для обмена электронными сообщениями (на этапе отправки сообщения его автором)	25 (*TCP*)
POP3 (Post Office Protocol)	«Протокол почтового отделения»; довольно простой протокол, используемый почтовым клиентом (например, программой *Outlook Express*) для подключения к своему почтовому ящику на сервере и считывания сообщений (на этапе доставки почтового сообщения адресату)	110 (*TCP*)
IMAP4 (Internet Message Access Protocol)	Протокол доступа к электронным сообщениям – более функциональный, чем *POP*3, клиентский протокол для доступа к почтовому серверу	143 (*TCP*)
SSL (Secure Sockets Layer)	Протокол, обеспечивающий согласование алгоритмов и обмен ключами шифрования. Используется для защиты данных при их пересылке по сетям	25 (*SMTP*) 995 (*POP*3*S*) 993 (*IMAPS*) 443 (*HTTPS*) (*TCP*)

Чтобы посмотреть, какие порты на компьютере пользователя используются или ожидают подключения, достаточно выполнить команду *NETSTAT-AN*.

14.1.6. Адресация в IP-сетях

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

Физический, или локальный, адрес узла определяется 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-A0-17-3*D*-*BC*-01. Такие адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. 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 байтов (например, 109.26.17.100), 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 устанавливается 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.

Символьный адрес, или DNS-имя (в частности, *SERV*1.*IBM.COM*), назначается администратором и состоит из нескольких частей: имени машины, имени организации, имени домена и т. д. Такой адрес используется на прикладном уровне, например, в протоколах *FTP* или *Telnet*.

14.1.7. Протоколы сопоставления адреса ARP и RARP

Для определения локального адреса по *IP*-адресу используется протокол разрешения адреса *Address Resolution Protocol (ARP). 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.

14.1.8. Протокол ICMP

Протокол управления сообщениями *Internet* (*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.

14.1.9. Протокол IGMP

Узлы локальной сети используют протокол управления группами *Internet* (*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.

14.1.10. Протокол NDIS

Network Device Interface Specification – 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.

14.1.11. 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.

14.2. Настройка *IP*-адресации и маршрутизации

14.2.1. Основы IP-адресации

Первый обязательный параметр в свойствах протокола *TCP/IP* любого компьютера – его *IP*-адрес.

IP-адрес – это уникальная последовательность двоичных цифр, с помощью которой ПК однозначно идентифицируется в *IP*-сети. Напомним, что на канальном уровне в роли таких же уникальных адресов компьютеров выступают *MAC*-адреса сетевых адаптеров, невозможность совпадения которых контролируется изготовителями на стадии производства.

Существуют две версии протокола *IP – IPv4* и *IPv6*. В версии *IPv4 IP*-адрес представляется в виде 32-битной последовательности двоичных цифр, в *IPv6* – 128-битной.

Принятый сейчас 32-битный стандарт обеспечивает количество *IP*-адресов, равное почти 4,3 млрд, но их большая часть закреплена за США (около 70 %), Канадой и европейскими странами, а вот, например КНР, получила их всего 22 млн.

Новая 128-разрядная версия протокола *IPv6* позволит увеличить количество *IP*-адресов до величины – $3{,}4 \times 10^{38}$.

Для использования протокола *IPv6* в некоторых версиях ОС *Windows* имеется необходимое программное обеспечение, которое по умолчанию не активизировано. Чтобы задействовать новый протокол, надо в командной строке (меню Пуск/Выполнить) ввести и запустить на исполнение команду «*ipv6 install*». Получить необходимые справки по работе с протоколом *IPv6* можно командой «*ipv6*/*?*».

Для удобства работы с *IP*-адресами 32-разрядную последовательность обычно разделяют на четыре части по 8 бит (на *октеты),* каждый октет переводят в десятичное число и при записи разделяют эти числа

точками. В таком виде (это представление называется «десятичные числа с точками», или, по-английски, *«dotted-decimal notation»)* *IP*-адреса занимают гораздо меньше места и намного легче запоминаются (табл. 14.2).

Табл. 14.2. Различные представления *IP*-адреса

IP-адрес в 32-разрядном виде	11000000 10101000 0000101 11001000			
IP-адрес, разбитый на октеты	11000000	10101000	0000101	11001000
Октеты в десятичном представлении	192	168	5	200
IP-адрес в виде десятичных чисел, разделенных точками	192.168.5.200			

Однако одного только *IP*-адреса компьютеру для работы в сети *TCP/IP* недостаточно. Второй обязательный параметр, без которого протокол *TCP/IP* работать не будет, – *маска подсети.*

Маска подсети – это 32-разрядное число, состоящее из идущих вначале единиц, а затем – нулей, например 255.255.255.0 (в десятичном представлении).

Маска подсети играет важную роль в *IP*-адресации и маршрутизации. Для правильного взаимодействия в сложной сети участники должны уметь определять, какие *IP*-адреса принадлежат его *локальной* сети, а какие – *удаленным* сетям.

Здесь и используется маска подсети, с помощью которой производится *разделение любого IP*-адреса на две части: *идентификатор сети (Net ID)* и *идентификатор узла (Host ID).* Такое разделение делается очень просто: там, где в маске подсети стоят единицы, находится идентификатор сети, а где стоят нули – идентификатор узла.

Например, в *IP*-адресе 192.168.5.200 при использовании маски 255.255.255.0 идентификатором сети будет 192.168.5.0, а узла – 200. Для маски 255.255.0.0 сеть – 192.168.0.0 и узел – 5.200.

Правила назначения IP-адресов сетей и узлов:

1. Идентификатор сети не может содержать только двоичные нули или только единицы. Например, адрес 0.0.0.0 не может являться идентификатором сети.

2. Идентификатор узла также не может содержать только двоичные нули или только единицы – такие адреса зарезервированы для специальных целей.
3. Все нули в идентификаторе узла означают, что этот адрес является *адресом сети.* Например, 192.168.5.0 – правильный адрес сети при использовании маски 255.255.255.0 и его нельзя использовать для адресации ПК.
4. Все единицы в идентификаторе узла означают, что этот адрес является *адресом широковещания* для данной сети. Например, 192.168.5.255 – адрес широковещания в сети 192.168.5.0 при использовании маски 255.255.255.0 и его нельзя использовать для адресации компьютеров.
5. Идентификатор узла в пределах одной и той же подсети должен быть уникальным.
6. Диапазон адресов от 127.0.0.1 до 127.255.255.254 нельзя использовать в качестве *IP*-адресов компьютеров. Вся сеть 127.0.0.0 по маске 255.0.0.0 зарезервирована под так называемый *«адрес заглушки» (loopback),* используемый в *IP* для обращения компьютера к самому себе.

Это легко проверить: достаточно на любом компьютере с установленным протоколом *TCP*/*IP* выполнить команду *PING* 127.12.34.56, и, если протокол *TCP*/*IP* работает, вы увидите, как ваш компьютер будет отвечать на собственные запросы.

14.2.2. Классовая и бесклассовая IP-адресация

Первоначальная система *IP*-адресации в *Internet* выглядела следующим образом. Все пространство возможных *IP*-адресов (а это более четырех миллиардов, точнее 4 294 967 296 адресов) было разбито на *пять классов,* причем принадлежность *IP*-адреса к определенному классу определялась по нескольким битам первого октета (табл. 14.3). Заметим, что для адресации сетей и узлов использовались только классы *A*, *B* и *C*. Кроме того, для этих сетей были определены *фиксированные маски подсети по умолчанию,* равные соответственно 255.0.0.0, 255.255.0.0 и 255.255.255.0, которые не только жестко определяли диапазон возможных *IP*-адресов узлов в таких сетях, но и механизм маршрутизации.

Табл. 14.3. Классы адресов в первоначальной схеме *IP*-адресации

Класс	Первые биты в октете	Возможные значения первого октета	Возможное число сетей	Возможное число узлов в сети
A	0	1 – 126	126	16777214
B	10	128 – 191	16384	65534
C	110	192 – 223	2097152	254
D	1110	224 – 239	Используется для многоадресной рассылки (*multicast*)	
E	1111	240 – 254	Зарезервирован как экспериментальный	

Распределением *IP*-адресов в мире занимается частная некоммерческая корпорация под названием *ICANN* (*Internet Corporation for Assigned Names and Numbers*), а точнее, работающая под ее патронажем организация *IANA* (*Internet Assigned Numbers Authority*).

Чтобы рассчитать максимально возможное количество узлов в любой *IP*-сети, достаточно знать, сколько битов содержится в идентификаторе узла, или, иначе, сколько нулей имеется в маске подсети. Это число используется в качестве показателя степени 2, а затем из результата вычитаются два зарезервированных адреса (сети и широковещания). Аналогично легко вычислить и возможное количество сетей классов *A, B, C*, если учесть, что первые биты в октете уже зарезервированы, а в классе *A* нельзя использовать *IP*-адреса 0.0.0.0 и 127.0.0.0 для адресации сети.

Для получения нужного диапазона *IP*-адресов организациям предлагалось заполнить регистрационную форму, в которой следовало указать текущее число компьютеров и планируемый рост компьютерного парка в течение двух лет.

Первоначально данная схема хорошо работала, поскольку количество сетей было небольшим. Однако с развитием *Internet* такой подход к распределению *IP*-адресов стал вызывать проблемы, особенно острые для сетей класса *B*.

Действительно, организациям, в которых число компьютеров не превышало нескольких сотен (например, 500), приходилось регистрировать для себя целую сеть класса *B*. Поэтому количество доступных сетей класса *B* стало на глазах «таять», но при этом громадные диапазоны *IP*-адресов (в нашем примере – более 65000) пропадали зря.

Чтобы решить проблему, была разработана *бесклассовая схема IP-адресации (Classless InterDomain Routing, CIDR),* в которой не только отсутствует привязка *IP*-адреса к классу сети и маске подсети по умолчанию, но и допускается применение так называемых *масок подсети с переменной длиной (Variable Length Subnet Mask, VLSM).*

Например, если при выделении сети для вышеуказанной организации с 500 компьютерами вместо фиксированной маски 255.255.0.0 использовать маску 255.255.254.0, то получившегося диапазона из 512 возможных *IP*-адресов будет вполне достаточно.

Оставшиеся 65 тысяч адресов можно зарезервировать на будущее или раздать другим желающим подключиться к *Internet*.

Этот подход позволил гораздо более эффективно выделять организациям нужные им диапазоны *IP*-адресов, и проблема с нехваткой *IP*-сетей и адресов стала менее острой.

14.2.3. IP-адреса для локальных сетей

Все используемые в *Internet* адреса, как мы уже говорили, должны регистрироваться в *IANA*, что гарантирует их уникальность в масштабе всей планеты. Такие адреса называют *реальными,* или *публичными (public) IP*-адресами.

Для локальных сетей, не подключенных к *Internet*, регистрация *IP*-адресов, естественно, не требуется, так что в принципе здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможных конфликтов при последующем подключении такой сети к *Internet*, *RFC* 1918 рекомендует применять в локальных сетях только следующие диапазоны так называемых *частных (private) IP-адресов* (в *Internet* эти адреса не существуют и использовать их там нет возможности):

- 10.0.0.0-10.255.255.255;
- 172.16.0.0-172.31.255.255;
- 192.168.0.0-192.168.255.255.

14.2.4. Основы IP-маршрутизации

Как уже говорилось, чтобы правильно взаимодействовать с другими компьютерами и сетями, каждый ПК определяет, какие *IP*-адреса принадлежат его локальной сети, а какие – удаленным сетям. Если

выясняется, что *IP*-адрес компьютера назначения принадлежит локальной сети, пакет посылается непосредственно компьютеру назначения, если же это адрес удаленной сети, то пакет посылается по адресу основного шлюза.

Рассмотрим этот процесс подробнее. Возьмем, например, компьютер со следующими параметрами протокола *IP*:

- *IP*-адрес – 192.168.5.200;
- маска подсети – 255.255.255.0;
- основной шлюз – 192.168.5.1.

При запуске протокола *IP* на компьютере выполняется операция логического «И» между его собственными *IP*-адресом и маской подсети, в результате которой все биты *IP*-адреса, соответствующие нулевым битам маски подсети, также становятся нулевыми:

- *IP*-адрес в 32-разрядном виде –11000000 10101000 00000101 11001000;
- маска подсети – 11111111 11111111 11111111 00000000;
- идентификатор сети – 11000000 10101000 00000101 00000000.

Эта простая операция позволяет компьютеру определить *идентификатор собственной сети* (в нашем примере – 192.168.5.0).

Теперь предположим, что компьютеру надо отправить *IP*-пакет по адресу 192.168.5.15. Чтобы решить, как это нужно сделать, компьютер выполняет операцию логического «И» с *IP*-адресом компьютера назначения и собственной маской подсети. Легко понять, что полученный в результате *идентификатор сети назначения* будет совпадать с идентификатором собственной сети компьютера-отправителя. Так наш компьютер определит, что компьютер назначения находится в одной с ним сети, и выполнит следующие операции:

- с помощью протокола *ARP* будет определен физический *MAC*-адрес, соответствующий *IP*-адресу компьютера назначения;
- с помощью протоколов канального и физического уровня по этому *MAC*-адресу будет послана нужная информация.

Теперь посмотрим, что изменится, если пакет надо отправить по адресу 192.168.10.20. Компьютер выполнит аналогичную процедуру определения идентификатора сети назначения. В результате будет получен адрес 192.168.10.0, не совпадающий с идентификатором сети компьютера-отправителя. Так будет установлено, что компьютер назначения находится в удаленной сети, и алгоритм действий компьютера-отправителя изменится:

- будет определен *MAC*-адрес не компьютера назначения, а маршрутизатора;
- с помощью протоколов канального и физического уровня по этому *MAC*-адресу на маршрутизатор будет послана нужная информация.

Несмотря на то что *IP*-пакет в этом случае не доставляется непосредственно по назначению, протокол *IP* на компьютере-отправителе считает свою задачу выполненной. Дальнейшая судьба *IP*-пакета зависит от правильной настройки маршрутизаторов, объединяющих сети 192.168.5.0 и 192.168.10.0.

В данном примере легко продемонстрировать, насколько важна правильная настройка маски подсети в параметрах *IP*-адресации. Пусть мы по ошибке указали для компьютера 192.168.5.200 маску подсети, равную 255.255.0.0. В этом случае при попытке послать пакет по адресу 192.168.10.20 наш компьютер посчитает, что компьютер назначения находится в его собственной сети (ведь идентификаторы сетей при такой маске совпадают!), и будет пытаться отправить пакет самостоятельно.

В итоге этот пакет не попадет в маршрутизатор и не будет доставлен по назначению.

Чтобы понять, как работают маршрутизаторы, давайте сначала проанализируем *таблицу маршрутов,* которую выстраивает при загрузке протокола *IP* обычный компьютер, например с операционной системой *Windows XP* (рис. 14.2).

```
C:\>route print
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 11 09 13 0f 0e ...... Realtek RTL8139 Family PCI Fast Ethernet NIC - |
шэшяюЁЄ ярэшЁют·шър ярък€ют
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети       Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      192.168.5.1   192.168.5.200       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
      192.168.5.0  255.255.255.0  192.168.5.200   192.168.5.200       20
    192.168.5.200  255.255.255.255        127.0.0.1       127.0.0.1       20
    192.168.5.255  255.255.255.255  192.168.5.200   192.168.5.200       20
        224.0.0.0        240.0.0.0  192.168.5.200   192.168.5.200       20
  255.255.255.255  255.255.255.255  192.168.5.200   192.168.5.200        1
Основной шлюз:        192.168.5.1
===========================================================================
Постоянные маршруты:
  Отсутствует

C:\>_
```

Рис. 14.2. Таблица маршрутов в *Windows XP*

Как нетрудно видеть, в таблице определено несколько маршрутов с разными параметрами. Читать каждую такую запись в таблице маршрутизации нужно следующим образом:

Чтобы доставить пакет в сеть с адресом из поля «Сетевой адрес» и маской из поля «Маска сети», нужно с интерфейса с IP-адресом из поля «Интерфейс» послать пакет по IP-адресу из поля «Адрес шлюза», а «стоимость» такой доставки будет равна числу из поля «Метрика».

Отметим, что параметры «*Сетевой адрес»* и «*Маска сети»* вместе задают диапазон всех разрешенных в данной сети *IP*-адресов. Например, 127.0.0.0 и 255.0.0.0, как мы уже говорили, означают любой *IP*-адрес от 127.0.0.1 до 127.255.255.254. Вспомним также, что *IP*-адрес 127.0.0.1 называется «адресом заглушки» – посланные по этому адресу пакеты должны обрабатываться самим компьютером. Кроме того, маска 255.255.255.255 означает сеть из одного *IP*-адреса, а комбинация 0.0.0.0 – любой неопределенный адрес или маску подсети.

Тогда строка 1 в таблице маршрутизации означает в точности то, что делает компьютер при необходимости послать пакет в удаленную, т. е. неизвестную ему из таблицы маршрутизации, сеть – со своего интерфейса пакет посылается на *IP*-адрес маршрутизатора.

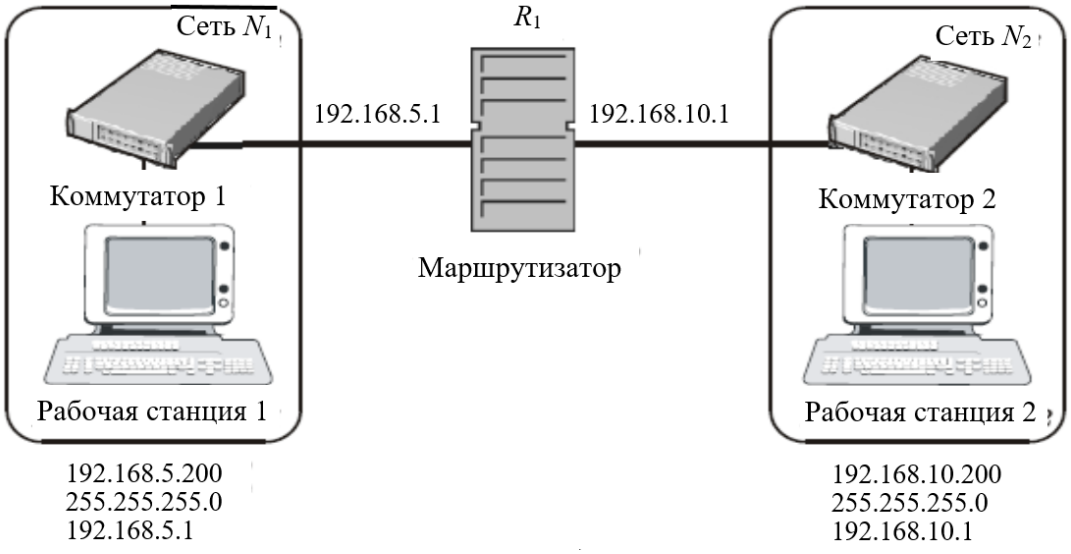
Строка 2 таблицы заставляет компьютер посылать самому себе (и отвечать на них) все пакеты, отправленные по любому *IP*-адресу из диапазона 127.0.0.1 – 127.255.255.254.

В строке 3 определено, как посылать пакеты компьютерам локальной сети по адресам из диапазона 192.168.5.1–192.168.5.254. Здесь четко видно, что делать это должен сам компьютер – адресом шлюза является его собственный *IP*-адрес 192.168.5.200.

Аналогично (5-я, 6-я и 7-я строки таблицы) нужно поступать и в случае, когда пакеты направляются по адресу рассылки подсети (192.168.5.255), по адресам многоадресной рассылки (224.0.0.0) или по адресу локальной широковещательной рассылки (255.255.255.255).

Строка 4 означает, что пакеты, посланные по *IP*-адресу 192.168.5.200 (обратите внимание на маску!), должны обрабатываться самим компьютером.

Несколько сложнее будет выглядеть таблица маршрутизации компьютера с двумя сетевыми адаптерами, который мы будем использовать в качестве маршрутизатора для объединения двух сегментов небольшой сети (рис. 14.3).



а)

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
        192.168.5.0  255.255.255.0  192.168.5.1  192.168.5.1  20
        192.168.5.1  255.255.255.255  127.0.0.1  127.0.0.1  20
      192.168.5.255  255.255.255.255  192.168.5.1  192.168.5.1  20
       192.168.10.0  255.255.255.0  192.168.10.1  192.168.10.1  20
       192.168.10.1  255.255.255.255  127.0.0.1  127.0.0.1  20
     192.168.10.255  255.255.255.255  192.168.10.1  192.168.10.1  20
          224.0.0.0        240.0.0.0  192.168.5.1  192.168.5.1  20
          224.0.0.0        240.0.0.0  192.168.10.1  192.168.10.1  20
    255.255.255.255  255.255.255.255  192.168.5.1  192.168.5.1  1
    255.255.255.255  255.255.255.255  192.168.10.1  192.168.10.1  1
```

б)

Рис. 14.3. Объединение сети с помощью маршрутизатора (*а*)
и таблица маршрутизации ПК *R*1 (*б*)

В этой таблице появилось несколько дополнительных строк, обозначающих маршруты в обе сети – 192.168.5.0 и 192.168.10.0. Заметим, что все такие маршруты будут выстроены компьютером автоматически.

Чтобы после этого наладить обмен *IP*-пакетами между сетями, нужно выполнить следующие действия:

- включить маршрутизацию на компьютере R_1 – это можно сделать, например, настроив службу маршрутизации и удаленного доступа, входящую в состав операционной системы *Windows Server* 2003;
- на всех компьютерах в сети N_1 параметр «Основной шлюз» нужно установить равным *IP*-адресу интерфейса маршрутизатора, подключенного к этой сети, т.е. равным 192.168.5.1, а на компьютерах в сети N_2 – равным 192.168.10.1.

Таким образом, маршрутизатор – это программно-аппаратное устройство с несколькими сетевыми интерфейсами, на котором работает *служба маршрутизации.*

Усложним нашу сеть, добавив в нее второй маршрутизатор и сеть N_3 с адресом 192.168.15.0 (рис. 14.4).

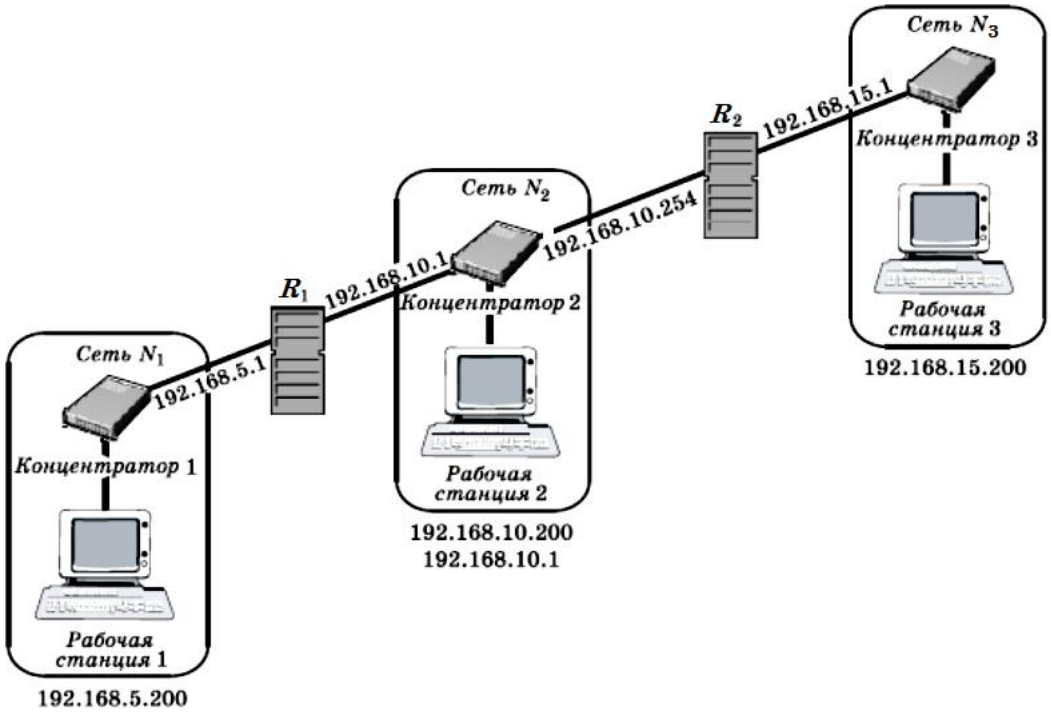


Рис. 14.4. Сеть с двумя маршрутизаторами

В такой сети настройка маршрутизации усложняется. Проблема в том, что, хотя маршрутизатор R_1 «знает», как посылать пакеты в сети N_1 и N_2, маршрута в сеть N_3 у него нет. В свою очередь, у маршрутизатора R_2 отсутствует маршрут в сеть N_1. Значит, обмен *IP*-пакетами между сетями N_1 и N_3 будет невозможен.

Решить эту проблему в такой небольшой сети довольно просто – надо добавить нужные записи в таблицы маршрутизаторов R_1 и R_2.

Для этого на маршрутизаторе R_1 достаточно выполнить команду, предписывающую направлять все пакеты, предназначенные для сети 192.168.15.0, по адресу 192.168.10.254 (т.е. 2-му маршрутизатору, который уже сможет доставить эти пакеты по назначению; ключ *P* используется, чтобы сделать этот маршрут постоянным):

ROUTE -P ADD 192.168.15.0

MASK 255.255.255.0 192.168.10.254

В качестве *IP*-адреса маршрутизатора принято выбирать либо первый, либо последний из возможных в данной *IP*-сети адресов.

Аналогичная команда на маршрутизаторе R_2 должна выглядеть так:

ROUTE -P ADD 192.168.5.0

MASK 255.255.255.0 192.168.10.1

После этого взаимодействие в нашей сети будет налажено.

В крупных сетях, содержащих большое количество соединенных друг с другом подсетей, вручную прописывать маршруты доставки пакетов на всех маршрутизаторах довольно утомительно. К тому же такие маршруты являются *статическими,* значит, при каждом изменении конфигурации сети нужно будет проделывать большую работу по перестройке системы *IP*-маршрутизации.

Чтобы избежать этого, достаточно настроить маршрутизаторы так, чтобы они обменивались друг с другом информацией о маршрутах. Для этого в локальных сетях используют такие протоколы, как *RIP (Routing Information Protocol)* и *OSPF (Open Shortest Path First).* Протокол *RIP* проще в настройке, чем *OSPF*, однако для обмена информацией в нем применяются широковещательные сообщения, заметно нагружающие сеть. Поэтому *RIP* обычно используют в относительно небольших сетях. Протокол *OSPF* работает эффективнее, но сложнее настраивается, поэтому его использование рекомендуется для крупных корпоративных сетей.

14.2.5. Назначение IP-адресов и проверка работоспособности TCP/IP

Самый простой способ настройки параметров протокола *IP* – назначать их вручную. Достоинством такого метода является то, что сетевые администраторы полностью контролируют все *IP*-адреса компьютеров в сети, что может быть важно с точки зрения защиты данных или взаимодействия с *Internet*. Однако у этого способа много недостатков. Во-первых, легко ошибиться и ввести неправильные параметры маски или шлюза или, что еще хуже, назначить повторяющийся в сети *IP*-адрес. Во-вторых, при изменениях параметров *IP*-адресации в сети (например, при смене *IP*-адреса маршрутизатора) придется перенастраивать все компьютеры. Но самое неприятное, что при таком способе настройки практически невозможно работать в крупных корпоративных сетях с мобильными устройствами типа ноутбуков или КПК, которые часто перемещаются из одного сегмента сети в другой.

Поэтому в организациях чаще применяют специальные серверы, поддерживающие протокол динамической конфигурации узлов *DHCP (Dynamic Host Configuration Protocol),* задача которых состоит в обслуживании запросов клиентов на получение *IP*-адреса и другой информации, необходимой для правильной работы в сети. Именно поэтому компьютеры с операционными системами *Windows* по умолчанию настроены на автоматическое получение *IP*-адреса.

Если сервер *DHCP* недоступен, то начиная с версии *Windows* 98 ПК самостоятельно назначают себе *IP*-адрес. При этом используется механизм автоматической личной *IP*-адресации *(Automatic Private IP Addressing, APIPA),* для которого корпорацией *Microsoft* зарегистрирован диапазон адресов 169.254.0.0 –169.254.255.255.

Для проверки параметров и работоспособности протокола *IP* необходимо:

1. Выполнить команду IPCONFIG /ALL.

При этом:

- если в выданной на экран информации не содержится никаких параметров, значит, нет активных интерфейсов;
- если в выданной информации есть диагностическое сообщение «Сеть отключена», значит, проблемы с физическим уровнем – проверьте подключение коннектора в разъеме сетевого адаптера и/или работоспособность коммутатора;
- если ваши параметры *IP*-адреса и маски подсети равны 0.0.0.0, значит, используется статический *IP*-адрес, конфликтующий с другим узлом в сети;
- если *IP*-адрес находится в диапазоне 169.254.*x.x*, значит, *DHCP*-сервер недоступен и работать можно только с теми компьютерами в сети, которые также самостоятельно назначили себе адрес.

В нормальной ситуации при получении *IP*-адреса от *DHCP*-сервера или правильной ручной настройке вы должны увидеть в выданной на экран информации такие параметры, как *IP*-адрес компьютера, маска подсети, основной шлюз, *DNS*-сервер и *DHCP*-сервер (а также, возможно, другие параметры).

2. Выполнить команду PING 127.0.0.1.

Если ответ не получен, это свидетельствует о неправильной настройке стека протоколов *TCP*/*IP*; придется переустановить соответствующую программную поддержку.

Если ответ получен, значит, стек протоколов *TCP*/*IP* работает правильно.

3. Выполнить команду PING w.x.y.z, где *w.x.y.z – IP-адрес соседнего ПК.*

Так проверяется работоспособность локальной сети.

4. Выполнить команду PING w.x.y.z, где *w.x.y.z – IP-адрес основного шлюза.*

Так проверяется доступность и работоспособность маршрутизатора.

5. Выполнить команду PING w.x.y.z, где *w.x.y.z – IP-адрес удаленного ПК.*

Так проверяется работоспособность всей системы маршрутизации вашей корпоративной сети или соединения с *Internet*.

Во многих современных сетях пакеты протокола *ICMP*, с помощью которых утилита *PING* тестирует взаимодействие, запрещаются по требованию служб безопасности. ОС *Windows SP*2 с включенным межсетевым экраном также блокирует *ICMP*-пакеты. Поэтому, если утилита *PING* не показывает ответов, не надо спешить искать причину «сбоя» на своем компьютере, а сначала необходимо выяснить у сетевого администратора (или в настройках ОС *Windows*), разрешено ли в сети использование *ICMP*.

В заключение приведем *набор кратких правил*, которые помогут не ошибиться при настройке *IP*-адресации и маршрутизации в сетях *TCP*/*IP*:

1) чтобы взаимодействовать в сети *TCP*/*IP*, все ПК должны иметь *IP*-адреса;

2) компьютеры, находящиеся в одном физическом сегменте сети (соединенные концентраторами или коммутаторами), должны принадлежать одной *IP*-сети, но иметь уникальные *IP*-адреса;

3) для определения идентификаторов локальной сети или удаленных сетей используется маска подсети;

4) чтобы взаимодействовать с удаленными сетями, компьютерам требуется адрес основного шлюза, который должен совпадать с адресом маршрутизатора, соединяющего вашу сеть с другими;

5) маршрутизаторы – это компьютеры с несколькими сетевыми интерфейсами, умеющие передавать *IP*-пакеты из одной сети в другую в соответствии со своими таблицами маршрутизации;

6) маршрутизатор всегда имеет маршруты во все сети, подключенные к нему непосредственно;

7) маршруты в другие сети нужно настраивать;

8) таблицы маршрутизации можно настраивать вручную либо применять динамические протоколы обмена информацией о маршрутизации.

14.3. Протоколы передачи данных нижнего уровня

Протоколы передачи данных нижнего уровня (протоколы управления каналом) – это совокупность процедур, выполняемых на двух нижних (*физическом и канальном)* уровнях семиуровневой эталонной модели ВОС.

На этих уровнях стек *OSI* поддерживает спецификации *Ethernet* (*OSI*-8802.3, *IEEE*-802.3), *Token Bus* (*OSI*-8802.4, *IEEE*-802.4), *Token Ring* (*OSI*-8802.4, *IEEE*-802.4), *FDDI* (*ISO*-9314), а также протоколы *LLC, X*.25, *ISDN* и *TCP/IP*.

Существует деление протоколов, которое определяется по уровню взаимодействия между передающим и приемным узлами (рис. 14.5):

1) протоколы типа первичный-вторичный;

2) равноранговые протоколы.

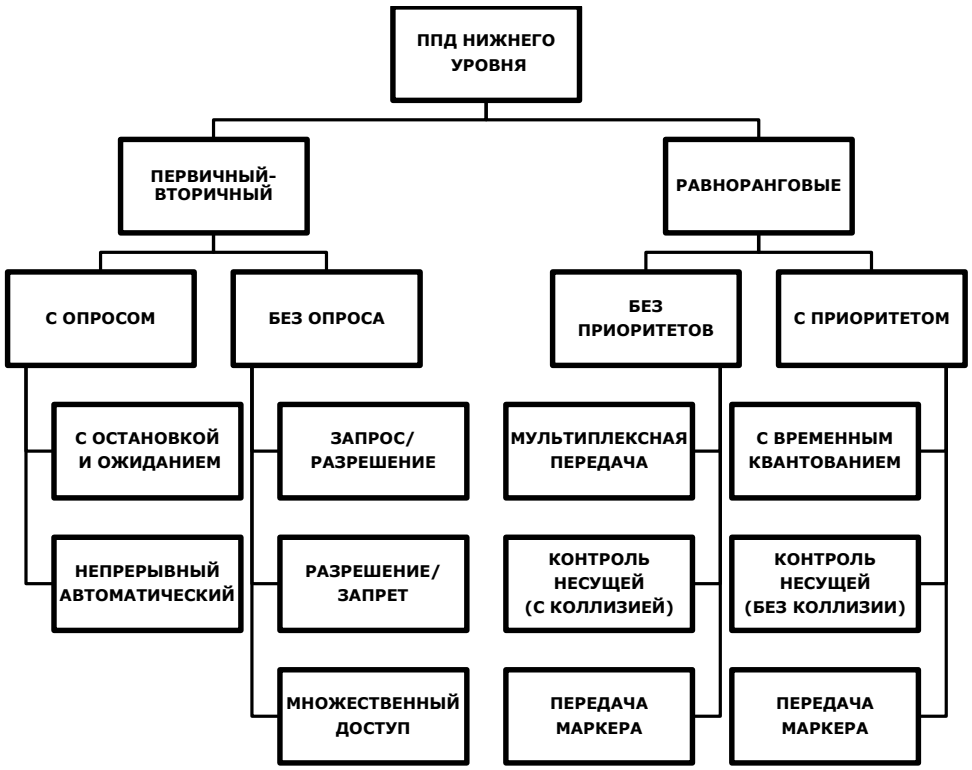


Рис. 14.5. Деление протоколов передачи данных нижнего уровня

В протоколах *типа первичный-вторичный* в явном виде присутствует главный узел, который управляет всеми остальными вторичными узлами, т.е. определяет, когда и какие узлы могут производить обмен данными. В равноранговых (одноранговых, одноуровневых) протоколах нет ярко выраженного главного узла (все они имеют одинаковый статус), и в каждый момент времени образуется новая пара первичный-вторичный.

Но если предварительно узлам присвоить разные приоритеты, то для них устанавливается неравный доступ.

Первичный узел – это узел, который инициирует передачу; вторичный – это узел, который принимает.

Протокол, использующий опрос с остановкой и ожиданием, реализует следующую схему: опрос вторичных узлов проходит, начиная с самого удаленного вторичного узла. Если узел готов к передаче, то он передает свои данные. Если данных нет, то опрашивается следующий узел и этот процесс повторяется до тех пор, пока не будут опрошены все узлы сети.

Более эффективные – протоколы типа непрерывного автоматического запроса на повторение (протоколы *ARQ*). В них устанавливаются «окна приема и передачи», или «временные интервалы». Внутри этих временных интервалов размещаются несколько непрерывно следующих друг за другом кадров данных. Подтверждение приема обеспечивается не для отдельного кадра, а для всего «окна» в целом.

За счет использования «окон» сокращается время, используемое на служебные операции. Чем больше ширина «окна», тем меньше служебное время.

Недостатком такого протокола является то, что для хранения кадров, переданных в «окно», необходимо буферное запоминающее устройство. При широких окнах возникает опасность переполнения окна и, следовательно, потеря данных.

Все протоколы с опросом объединяет идея: инициатива передачи принадлежит первичному узлу.

Первые из двух *протоколов без опроса* реализуют селективные методы доступа. А третий тип использует принцип резервирования времени.

Протоколы типа *запрос-разрешение* применяются в полудуплексных сетях, когда передача по разным направлениям ведется в разные

моменты времени. Источник сообщения (вторичный узел) генерирует сигнал запроса, и этот сигнал поступает на первичный узел. Если первичный узел разрешил передачу, то он соответствующим сигналом информирует об этом вторичный узел, вторичный узел начинает передачу.

В случае необходимости первичный узел запрещает передачу в любой момент времени (используется очень редко).

Протокол *разрешение-запрещение* имеет частный характер, применяется для работы, если оборудование вторичного узла имеет низкую пропускную способность.

Множественный доступ с временным разделением (Time Division MultIPle Access – TDMA) широко используется в спутниковых сетях связи.

Доступ *TDMA* основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Структура множественного доступа с разделением во времени показана на рис. 14.6.

Каждый из циклов начинается сигналом *Разграничитель* (Р). Цикл включает *N* пронумерованных временных интервалов, называемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.

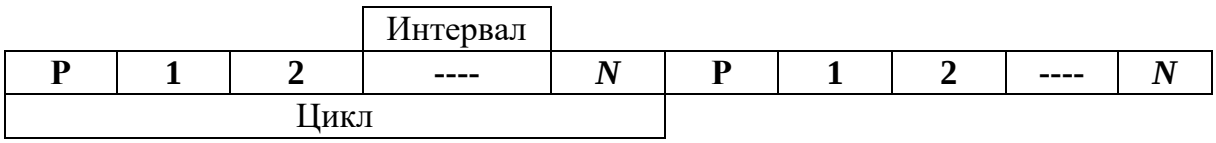


Рис. 14.6. Структура множественного доступа с разделением во времени

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

Первый (простейший) вариант использования интервалов заключается в том, что их число (*N*) выполняется 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.

К рассматриваемой группе протоколов типа «запрос-разрешение», «разрешение-запрещение» может быть отнесен протокол, использующий маркерный доступ как в кольцевых сетях. Маркер выполняет функции сигналов разрешения и запрещения.

Протоколы без опроса более эффективны, чем протоколы с опросом, при условии, что вторичные узлы более активны для передачи.

Если вторичные узлы создают данные для передачи редко, то протоколы без опроса неэффективны, так как они более сложны. Если интенсивность создания данных высокая, то протоколы без опроса более эффективны.

В группе равноранговых протоколов может использоваться или не использоваться система приоритетов.

Если система приоритетов не используется, то все вторичные узлы равноправны. Им предоставляется одинаковое время для передачи. Вторичные узлы не могут инициировать процесс передачи.

Наиболее простая равноранговая *неприоритетная* система – *мультиплексная передача с временным разделением*, где реализуются методы доступа к передающей среде, основанные на резервировании времени. Здесь используется жесткое расписание работы абонентов: каждой станции выделяется интервал времени (слот) использования канала связи, и все интервалы распределяются поровну между станциями. Во время слота станция получает канал в свое полное распоряжение. Такой протокол отличается простотой в реализации и широко применяется в глобальных и локальных сетях. Недостатки протокола:

• возможность неполного использования канала, когда станция, получив слот, не может загрузить канал полностью из-за отсутствия необходимого объема данных для передачи;

• нежелательные задержки в передаче данных, когда станция, имеющая важную и срочную информацию, вынуждена ждать своего слота или когда выделенного слота недостаточно для передачи подготовленных данных и необходимо ждать следующего слота.

Суть протокола с контролем несущей и контролем столкновений (коллизий) (*Carrier Sense MultIPle Access with Collision Detection – CSMA/CD*) в том, что передающая абонентская система контролирует все время состояние канала, и если канал свободен, то система начинает передачу. Доступ на передачу абонентской системы здесь ничем не регламентируется, за исключением того, свободен он или занят. При этом используются два основных принципа:

• «слушай, прежде чем говорить» – если канал свободен, абонентская система подключается на передачу, и, по существу, как бы захватывает канал;

• «слушай, когда говоришь».

Алгоритм множественного доступа с прослушиванием несущей и разрешением коллизий приведен на рис. 14.7.

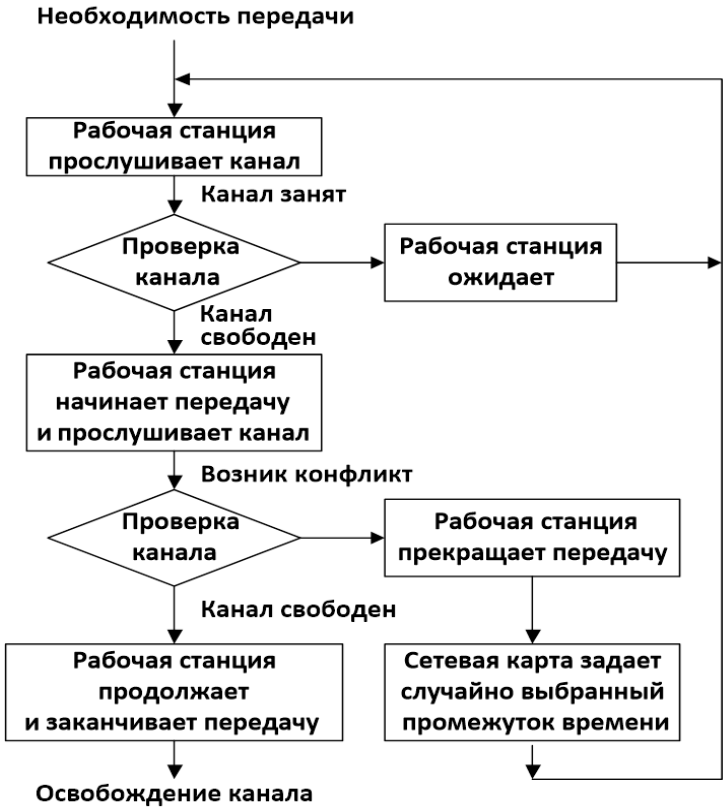


Рис. 14.7. Алгоритм множественного доступа
с прослушиванием несущей и разрешением коллизий

При возникновении конфликта из-за того, что два узла пытаются занять канал, 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.

Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени. Если конфликт возникнет во время повторной передачи сообщения, этот промежуток времени будет увеличен. Стандарт типа *Ethernet* определяет сеть с конкуренцией, в которой несколько рабочих станций должны конкурировать друг с другом за право доступа к сети.

Реализацией данного метода явилась технология *Ethernet,* разработанная в исследовательском центре компании *Xerox.*

Недостатком метода является то, что возможны коллизии (или столкновения) в канале, связанные с вероятностью наложения на этот сигнал других сигналов сети. Результат этого – искажение передаваемых сигналов, что в конечном итоге приводит к потере информации.

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

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

При использовании *множественного доступа с разделением длины волны* (*Wavelength Division MultIPle Access – WDMA*) широкая полоса пропускания канала делится на ряд узких полос длин волн, разделенных защитными полосами. В каждой узкой полосе создается логический канал.

В оптических каналах разделение частоты выполняется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При мультиплексировании в один световод свет излучается большим числом 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.

Равноранговые приоритетные системы представлены тремя подходами, реализованными в приоритетных слотовых системах:

- с приоритетами и временным квантованием;
- контролем несущей без коллизий;
- передачей маркера с приоритетами.

Приоритетные системы с временным квантованием (или слотовые системы) подобны бесприоритетным системам, в которых происходит мультиплексная передача с временным разделением. Однако канал используется здесь на приоритетной основе. В качестве критериев для установления приоритетов применяются следующие: предшествующее владение слотом; время ответа, которое удовлетворяет станцию-отправителя; объем передаваемых данных (чем меньше объем, тем выше приоритет) и др.

Недостатки протокола:

- данные должны передаваться строго определенной длины (в течение заданного слота они должны быть переданы);
- существует возможность простоя канала, присущая всем протоколам, которые реализуют методы доступа, основанные на резервировании времени.

В *системах с контролем несущей без коллизий* в отличие от аналогичных систем с коллизиями используется специальная логика для предотвращения коллизий. Каждая станция сети, в которой реализуется такая система обслуживания запросов, имеет дополнительное устройство – таймер или арбитр. Это устройство определяет, когда станция может вести передачу без опасности коллизий. Его особенностью является то, что они случайным образом устанавливаются в исходные положения (у каждого свое); генераторы тактовых импульсов для этих таймеров имеют свои установки частоты, которые также устанавливаются случайным образом.

Когда станции установили наличие столкновений, они запускают свои таймеры. Каждый таймер выполняет свой отчет времени, и тогда по командам таймера, когда произведен отчет времени, станция делает новую попытку передачи. Так как таймеры установлены случайным образом, то существует вероятность того, что станции проведут свои

передачи без столкновений. А если вновь зафиксируется столкновение, то процесс повторится. Главная станция для управления использованием канала не предусматривается.

Установка времени на таймере, по истечении которого станция может вести передачу данных, выполняется на приоритетной основе. Для станции с наивысшим приоритетом переполнение таймера наступает раньше. Если станция с высоким приоритетом не намерена вести передачу, канал будет находиться в состоянии покоя, т.е. свободен, и тогда следующая по приоритету станция может захватить канал.

Несколько особый механизм имеют приоритеты в *сетях с маркерным доступом (Token Passing MultIPle Access – TPMA).*

Магистральные сети, использующие этот метод, называются сетями типа «маркерная шина», а кольцевые сети – сетями типа «маркерное кольцо».

В сетях типа «*маркерная шина*» (рис. 14.8) доступ к каналу обеспечивается таким образом, как если бы канал был физическим кольцом, причем допускается использование канала не кольцевого типа (шинного, звездообразного).

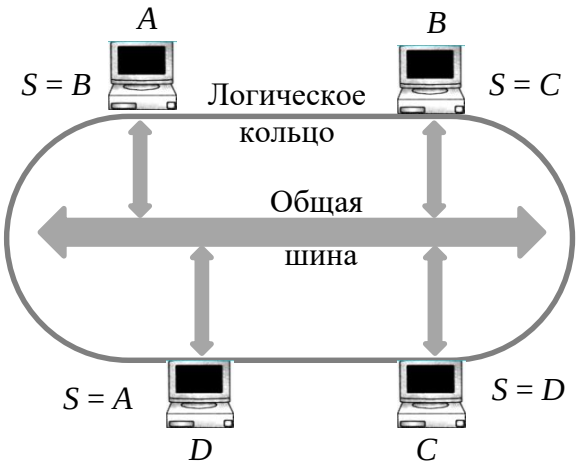


Рис. 14.8. Сеть типа «*маркерная шина*» (*S* – адрес следующей станции)

Право пользования каналом передается организованным путем. Маркер (управляющий кадр) содержит адресное поле, где записывается адрес станции, которой предоставляется право доступа в канал. Станция, получив маркер со своим адресом, имеет исключительное право на передачу данных (кадра) по физическому каналу. После передачи кадра станция отправляет маркер другой станции, которая является очередной по установленному порядку владения правом на передачу. Каждой станции известен идентификатор следующей станции. Станции получают маркер в циклической последовательности, при этом в физической шине формируется так называемое *логическое кольцо*. Все станции «слушают» канал, но захватить канал для передачи данных может только

та станция, которая указана в адресном поле маркера. Работая в режиме прослушивания канала, принять переданный кадр может только та станция, адрес *S* которой указан в поле адреса получателя этого кадра.

Преимущество такого метода в том, что не требуется физического упорядочения подключенных к шине станций, так как с помощью механизма логической конфигурации может быть обеспечен любой порядок передачи маркера станции.

Протокол типа «*маркерное кольцо*» (рис. 14.9) применяется в сетях с кольцевой топологией. В таких сетях сигналы распространяются через однонаправленные двухточечные пути между узлами. Узлы и однонаправленные звенья соединяются последовательно, образуя физическое кольцо. Как и в случае маркерной шины, в протоколе типа «маркерное кольцо» в качестве маркера используется уникальная последовательность битов. Однако маркер не имеет адреса. Он снабжается полем занятости, в котором записывается один из кодов, обозначающих состояние маркера – свободное или занятое. Если ни один из узлов сети не имеет данных для передачи, свободный маркер циркулирует по кольцу, совершая однонаправленное (обычно против часовой стрелки) перемещение. В каждом узле маркер задерживается на время, необходимое для его приема, анализа (с целью установления занятости) и ретрансляции.

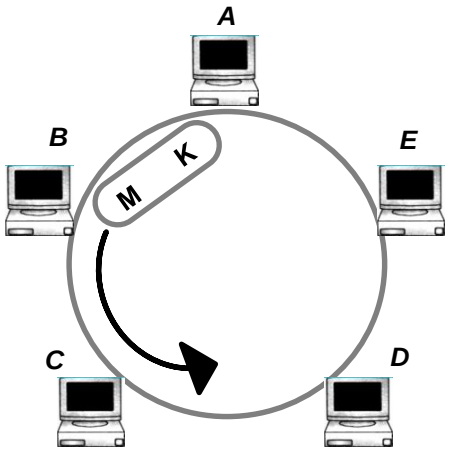


Рис. 14.9. Сеть «маркерное кольцо»: М – маркер; К – кадр

Свободный маркер означает, что кольцевой канал свободен, и любая станция, имеющая данные для передачи, может его использовать. Получив свободный маркер, станция, готовая к передаче кадра с данными, меняет состояние маркера на «занятый», передает его дальше по кольцу и добавляет к нему кадр.

Алгоритм множественного доступа с передачей полномочия, или маркера, приведен на рис. 14.10.

Рис. 14.10. Алгоритм множественного доступа с передачей маркера

При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по локальной вычислительной сети. Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция-адресат принимает его. При этом она создает новый маркер.

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 гарантирует определенное время доставки блоков данных в сети и дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу, кроме того, включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

Основные преимущества протокола типа «маркерное кольцо»:

- имеется возможность проверки ошибок при передаче данных: станция-отправитель, получив свой кадр от станции-получателя, сверяет его с исходным вариантом кадра. В случае наличия ошибки кадр передается повторно;
- канал используется полностью, его простои отсутствуют;
- имеется принципиальная возможность осуществлять одновременную передачу несколькими станциями сети.

Недостатки протокола:

- невозможность передачи кадров произвольной длины;
- не предусматривается использование приоритетов.

В *приоритетных системах с передачей маркера* устранены эти недостатки.

Здесь каждой станции сети определен свой уровень приоритета, причем, чем выше уровень приоритета, тем меньше его номер. Назначение приоритетной схемы состоит в том, чтобы дать возможность каждой станции зарезервировать использование канала для следующей передачи по кольцу.

Каждый узел анализирует перемещающийся по кольцу маркер, который содержит поле резервирования (ПР). Если собственный приоритет выше, чем значение приоритета в ПР маркера, станция увеличивает значение приоритета в ПР до своего уровня, резервируя тем самым маркер на следующий цикл. Если в данном цикле какой-то другой узел не увеличит еще больше значение уровня приоритета в ПР, этой станции разрешается использовать маркер и канал во время следующего цикла передачи по кольцу (за время цикла маркер совершает полный оборот по кольцу).

Чтобы запросы на обслуживание со стороны станций с низким приоритетом не были потеряны, станция, захватившая маркер, должна запомнить предыдущее значение ПР в своем ЗУ. После «высвобождения» маркера, когда он завершит полный оборот по кольцу, станция восстанавливает предыдущий запрос к сети, имеющий более низкий приоритет.

Таким образом, протоколы передачи данных нижнего уровня реализуют соответствующие методы доступа к передающей среде. При этом передаются сообщения (пакеты) между рабочими станциями, но не решаются вопросы, связанные с сетевыми файловыми системами и переадресацией файлов. Эти протоколы не включают никаких средств обеспечения правильной последовательности приема переданных данных и средств идентификации прикладных программ, нуждающихся в обмене данными.

14.4. Определение основных характеристик системы передачи данных

Рассмотрим простейшую цифровую сеть связи на базе протокола *TCP/IP*, состоящую из двух персональных компьютеров, соединенных между собой через *Hub* (рис. 14.11).

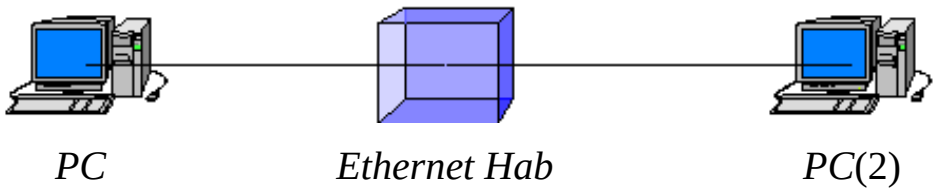


Рис. 14.11. Простая цифровая сеть связи

При расчете характеристик такой сети необходимо знать закон распределения длин передаваемых пакетов $\omega(x)$ и распределение интервалов времени между ними $\omega(t)$. Считается, что эти плотности распределения вероятностей (ПРВ) известны. Тогда можно определить среднюю длину передаваемых пакетов как математическое ожидание (МО):

$$m_x = \int x\omega(x)dx,$$

и средний интервал времени между двумя соседними пакетами

$$m_t = \int t\omega(t)dt\,,$$

В табл. 14.4 приведены наиболее часто используемые в цифровых системах ПРВ с их основными числовыми характеристиками.

Табл. 14.4. Часто используемые ПРВ в цифровых системах связи

Название закона распределения	Плотность распределения вероятностей $\omega(x)$	Моменты
Нормальный	$\frac{1}{\sqrt{2\pi\sigma}}\exp\left(-\frac{(x-a)^2}{2\sigma^2}\right)$	$m_1 = a$, $\mu_2 = \sigma^2$, $\mu_3 = 0$, $\mu_4 = 3\sigma^4$
Равномерный	$\frac{1}{b-a}, a \le x \le b$	$m_1 = \frac{a+b}{2}, \mu_2 = \frac{(b-a)^2}{12}$, $\mu_3 = 0, \mu_4 = \frac{1}{80}(b-a)^4$
Экспоненциальный	$\lambda e^{-\lambda e}, x \ge 0$	$m_1 = 1/\lambda\,, m_2 = 2/\lambda^2\,,$ $\mu_2 = 1/\lambda^2\,, \mu_3 = 2/\lambda^3\,,$ $\mu_4 = 9/\lambda^4$
Логарифмически-нормальный	$\frac{1}{x\sqrt{2\pi\sigma}}\exp\left(-\frac{(\ln x - a)^2}{2\sigma^2}\right), x > 0$	$m_1 = \exp(\alpha + 0{,}5\sigma^2)$, $\mu_2 = \exp(2a + \sigma^2)(\exp(\sigma^2) - 1)$
Гамма	$\frac{1}{\beta^\alpha \Gamma(\alpha)} x^{\alpha-1} e^{-x/\beta}, x \ge 0, \beta > 0$	$m_1 = \alpha\beta, m_2 = \alpha(\alpha+1)\beta^2$, $\mu_2 = \alpha\beta^2, \mu_3 = 2\alpha\beta^3$, $\mu_4 = 3(\alpha+2)\alpha\beta^4$
Вейбулла	$\alpha\beta x^{\alpha-1}\exp(-\beta x^\alpha),\ x \ge 0$	$m_1 = \Gamma\left(1+\frac{1}{\alpha}\right)\beta^{-1/\alpha}$ $\mu_2 = \left(\Gamma\left(1+\frac{2}{\alpha}\right) - \Gamma^2\left(1+\frac{1}{\alpha}\right)\right)\beta^{-2/\alpha}$

На основе величин m_x и m_t определяется средняя загруженность канала связи по формуле

$$\overline{\vartheta} = m_x/m_t = m_x\mu\,,$$

где $\mu = 1/m_t$ – интенсивность передачи пакета по каналу связи. Анализ данного выражения показывает, что загруженность линии связи зави-

сит как от размеров передаваемых пакетов, так и от интенсивности их генерации сетевой картой. Если величина $\overline{\vartheta} \geq \vartheta_{line}$, где ϑ_{line} – предельная скорость передачи данных по линии связи, то некоторые из переданных пакетов будут теряться с вероятностью

$$p_B = 1 - \frac{\vartheta_{line}}{\overline{\vartheta}}$$

Среднее время передачи пакета по каналу связи определяется по формуле

$$t_{\text{ср}} = \frac{m_x}{\vartheta_{line}} = \frac{1}{\mu},$$

где μ – интенсивность передачи пакетов по линии связи. Зная величины λ и μ, можно определить нагрузку в цифровой системе как

$$Z = \frac{\lambda}{\mu}.$$

Если цифровая система включает буфер с ограниченным объемом и роутер, то структурную схему такой системы можно представить в виде, изображенном на рис. 14.12.

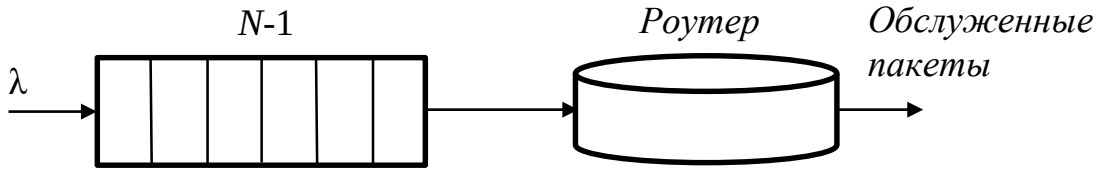


Рис. 14.12. Блок-схема системы с ограниченной длиной очереди и роутером

Входной поток со средней интенсивностью λ формируется первым компьютером и передается второму. Компьютеры связаны между собой через роутер, который имеет буфер входных и выходных данных. Задача роутера заключается в передаче поступивших пакетов второму ПК.

Допустим, что максимальное число пакетов в буфере роутера может быть равно *N*. Поступивший *N* +1 пакет получает отказ в обслуживании и считается потерянным.

Будем полагать, что интервалы времени между поступлениями пакетов распределены по экспоненциальному закону с параметром λ. Данный параметр считается известным до процесса моделирования и задается вариантом лабораторной работы. Для того чтобы время обслуживания было тоже подчинено экспоненциальному закону, необходимо

длины пакетов описывать экспоненциальным распределением. В этом случае время передачи пакетов, т. е. время их обслуживания $t = L/\vartheta_{line}$, где L – длина передаваемого пакета, будет также подчиняться экспоненциальному закону с параметром

$$\mu = 1/t_{ср},$$

где $t_{ср} = L_{ср}/\vartheta_{line}$ – среднее время передачи пакетов по каналу связи.

Сделанные допущения о моделях трафика позволяют использовать формулу Эрланга для систем с ограничением по длине очереди при вычислении вероятности нахождения пакетов в роутере:

$$p_k = \frac{\frac{Z^n}{n!}\left(\frac{Z}{n}\right)^{k-n}}{\sum_{j=0}^{n}\frac{Z^n}{n!} + \frac{Z^n}{n!}\sum_{s=0}^{N-1}\left(\frac{Z}{n}\right)^s},$$

где $Z = \lambda/\mu$ – величина нагрузки; n – число серверов. Так как в рассматриваемом случае $n = 1$, то формула упрощается до следующего выражения:

$$p_{k=1+s} = \frac{Z^k}{1 + Z + Z\sum_{s=1}^{N-1} Z^s} = Z^k\frac{1-Z}{1-Z^{N+1}} \quad \text{при } 0 \le k \le N$$

и $p_k = 0$ при $\kappa > N$.

Полученное выражение для p_k можно использовать при вычислении вероятности блокировки (потери пакета). Очевидно, что блокировки возникают при одновременном совершении двух событий: когда в роутере находится N пакетов и когда на его вход поступает $N + 1$ пакет. Вероятность первого события определяется как

$$p_{k=N} = \frac{Z^N(1-Z)}{1-Z^{N+1}}.$$

Учитывая, что входной поток является простейшим, вероятность второго события определяется по формуле

$$p^{(N+1)} = \lim_{S\to\infty}\frac{S-N}{S} = 1.$$

Вероятность потери пакета

$$p_B = p_N p^{(N+1)} = \frac{Z^N(1-Z)}{1-Z^{N+1}}.$$

Вероятность блокировки также можно выразить через интенсивность входного потока λ и интенсивность потока отброшенных пакетов R:

$$\mathrm{p}_B = \frac{R}{\lambda} \Longrightarrow R = \mathrm{p}_B\lambda.$$

Последнее выражение позволяет вычислять число потерянных пакетов за единицу времени. Среднее число пакетов в системе может быть найдено как математическое ожидание по следующей формуле:

$$\overline{N} = \sum_{k=0}^{N} p_k = \frac{(1-Z)Z}{1-Z^{N+1}} \sum_{k=0}^{N} Z^{k-1} = \frac{Z}{1-Z} - \frac{(N+1)Z^{N+1}}{1-Z^{N+1}},$$

а среднее время пребывания пакетов в системе как $T = \overline{N}/\lambda$.

Вопросы к компьютерному тестированию

1. Какой адрес компьютера в сетях назначается администратором во время конфигурирования компьютеров и маршрутизаторов?
2. Какие протоколы используются для определения локального адреса по *IP*-адресу, для контроля скорости передачи информации между двумя системами?
3. Какой протокол используется для регистрации себя в группе?
4. Какова разрядность представления адреса в версии протокола *IP* – *IPv*6?
5. Запишите численное значение идентификатора сети при *IP*-адресе 192.168.5.200 при использовании маски 255.255.255.0.
6. Запишите численное значение идентификатора узла при *IP*-адресе 192.168.5.200 при использовании маски 255.255.0.0.
7. Какая операция при выполнении маршрутизации позволяет компьютеру определить идентификатор собственной сети?
8. Какие операции будут выполнены в случае несовпадения идентификатора сети назначения с идентификатором собственной сети компьютера-отправителя?
9. Как называется протокол, обеспечивающий автоматическое получение *IP*-адреса?
10. Какую команду необходимо выполнить для проверки настройки стека протоколов *TCP*/*IP*?
11. В протоколах какого типа в явном виде присутствует и отсутствует ярко выраженный главный узел?
12. В каком из протоколов передачи данных нижнего уровня время простоя вторичных узлов определяется удалением их от первичных узлов?
13. В каком из протоколов передачи данных нижнего уровня устанавливаются «окна приема и передачи»?

14. В каких протоколах передачи данных нижнего уровня инициатива передачи принадлежит первичному узлу?
15. Протоколы какого типа обычно применяются в полудуплексных сетях?
16. Протоколы какого типа обычно применяются для работы, если оборудование вторичного узла имеет низкую пропускную способность?
17. Протоколы какого типа обычно используются в спутниковых сетях связи?
18. В каких случаях эффективность протоколов без опроса более высокая?
19. Какие из протоколов реализуют селективные методы доступа, а какие используют принцип резервирования времени?
20. В протоколах какого типа обычно все временные интервалы (слоты) распределяются поровну между станциями?
21. При каких методах доступа к передающей среде возможно возникновение коллизий?
22. Что такое «коллизия» сигналов?
23. Какие дополнительные устройства, устанавливаемые в сети, увеличивают вероятность осуществления передачи абонентских станций без коллизий?
24. Какому абонентскому узлу обычно устанавливается наиболее высокий приоритет?
25. В каких равноранговых приоритетных системах осуществляется мультиплексная передача с временным разделением?
26. В каких равноранговых приоритетных системах используется специальная логика или логическое кольцо для предотвращения коллизий?
27. Каково содержание маркера, используемого в сетях типа «маркерная шина», «маркерное кольцо»?
28. Какой порядок передачи маркера в сетях типа «маркерная шина», «маркерное кольцо»?
29. Какая последовательность действий характеризует работу принимающей рабочей станции при перемещении кадра по кольцу?
30. В каких равноранговых приоритетных системах имеется возможность проверки ошибок при передаче данных, передачи кадров произвольной длины?

Глава 15

ТОПОЛОГИИ И ТЕХНОЛОГИИ ПРОВОДНЫХ ЛВС

Рассматриваемые вопросы:

15.1. Сетевые топологии.
15.1.1. Шинная топология.
15.1.2. Топология типа «звезда».
15.1.3. Кольцевая топология.
15.1.4. Комбинированные топологии ЛКС.
15.2. Сетевые технологии.
15.2.1. Технология *Ethernet*.
15.2.2. *Fast Ethernet*.
15.2.3. Стандарт *Gigabit Ethernet*.
15.2.4. Технология *Token Ring*.
15.2.5. Технология *ARCnet*.
15.2.6. Технология *FDDI*.
15.2.7. Домашние сети на базе электропроводки.

15.1. Сетевые топологии

Топология компьютерной сети отражает структуру связей между ее основными функциональными элементами. При создании сети в зависимости от задач, которые она должна будет выполнять, могут быть реализованы одна или несколько из нижепредставленных трех базовых сетевых топологий.

15.1.1. Шинная топология

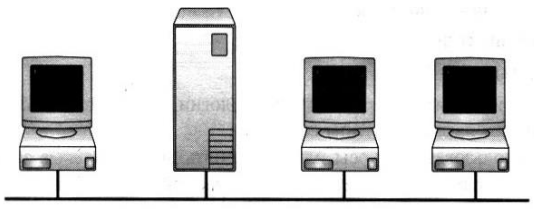


Рис. 15.1. Шинная топология

При шинной топологии среда передачи информации представляется в форме коммуникационного пути, доступного для всех рабочих станций, к которому они должны быть подключены (рис. 15.1). Все рабочие станции могут непосредственно вступать в контакт с любой рабочей станцией, имеющейся в сети.

Рабочие станции в любое время без прерывания работы всей вычислительной сети могут быть подключены к ней или отключены. Функционирование вычислительной сети не зависит от состояния отдельной рабочей станции.

В стандартной ситуации для шинной сети *Ethernet* часто используют тонкий кабель, или *Cheapernet*-кабель, с тройниковым соединителем. Выключение и особенно подключение к такой сети требуют разрыва шины, что вызывает нарушение циркулирующего потока информации и зависание системы.

Особенности использования шинной топологии

Электрические сигналы распространяются от одного конца кабеля к другому. Сигнал, достигая конца кабеля, будет отражаться и создавать помехи. На концах кабеля электрические сигналы необходимо гасить.

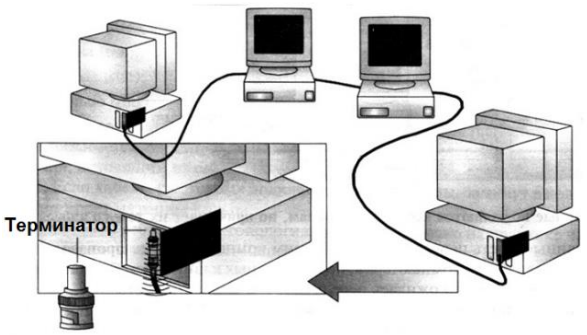


Рис. 15.2. Установка терминаторов в шинной топологии

Чтобы предотвратить отражение электрических сигналов, на каждом конце кабеля устанавливают терминаторы (*terminators*), поглощающие эти сигналы (рис. 15.2).

15.1.2. Топология типа «звезда»

Концепция топологии сети в виде звезды пришла из области больших ЭВМ, в которых головная машина получает и обрабатывает все данные с периферийных устройств как активный узел обработки данных. Этот принцип применяется в системах передачи данных, например в электронной почте *RELCOM*. Вся информация между двумя периферийными рабочими местами проходит через центральный узел вычислительной сети, которым может быть концентратор, файловый сервер и др. (рис. 15.3).

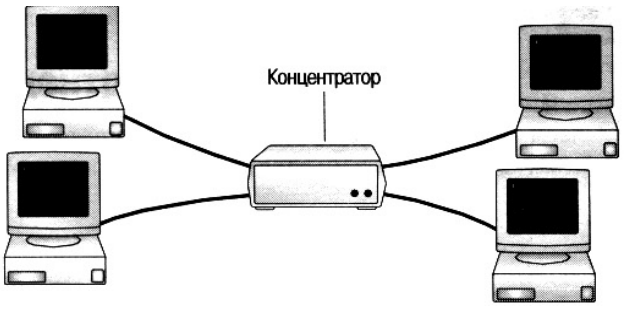


Рис. 15.3. Топология типа «звезда»

Пропускная способность сети определяется вычислительной мощностью узла и гарантируется для каждой рабочей станции. Коллизий (столкновений) данных не возникает.

Кабельное соединение довольно простое, так как каждая рабочая станция связана с узлом. Затраты на прокладку кабелей высокие, особенно когда центральный узел географически расположен не в центре топологии.

При расширении вычислительных сетей не могут быть использованы ранее выполненные кабельные связи: к новому рабочему месту необходимо прокладывать отдельный кабель из центра сети.

Топология в виде звезды – наиболее быстродействующая из всех топологий вычислительных сетей, поскольку передача данных между рабочими станциями проходит через центральный узел (при его хорошей производительности) по отдельным линиям, используемым только этими рабочими станциями. Частота запросов передачи информации от одной станции к другой невысокая по сравнению с достигаемой в других топологиях.

Производительность вычислительной сети в первую очередь зависит от мощности центрального файлового сервера. Он может быть узким местом вычислительной сети. В случае выхода из строя центрального узла нарушается работа всей сети.

Центральный узел управления – файловый сервер – может реализовать оптимальный механизм защиты против несанкционированного доступа к информации. Всей вычислительной сетью можно управлять из ее центра.

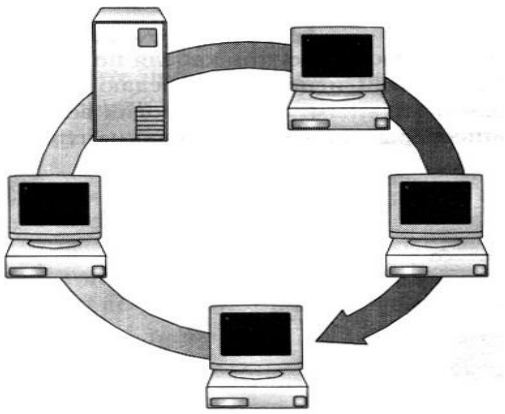


Рис. 15.4. Кольцевая топология

15.1.3. Кольцевая топология

При кольцевой топологии сети рабочие станции связаны одна с другой по кругу, и коммуникационная связь замыкается в кольцо (рис. 15.4).

При этом в основном используется метод передачи маркера, т.е. свободно циркулирующего по сети служебного пакета определенного формата, который имеет адресную часть и в который клиенты сети могут помещать свои информационные пакеты.

Пересылка сообщений является очень эффективной, так как большинство сообщений можно отправлять «в дорогу» по кабельной системе одно за другим. Очень просто можно сделать кольцевой запрос на все станции. Продолжительность передачи информации увеличивается пропорционально количеству рабочих станций, входящих в вычислительную сеть.

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. Неисправности в кабельных соединениях локализуются легко.

Прокладка кабелей от одной рабочей станции до другой может быть довольно сложной и дорогостоящей, особенно если географически рабочие станции расположены далеко от кольца (например, в линию).

Подключение новой рабочей станции требует краткосрочного выключения сети, так как во время установки кольцо должно быть разомкнуто. Ограничения на протяженность вычислительной сети не существует, так как она, в конечном счете, определяется исключительно расстоянием между двумя рабочими станциями.

15.1.4. Комбинированные топологии ЛКС

Наряду с известными топологиями вычислительных сетей «кольцо», «звезда» и «шина» на практике применяется и комбинированная, например древовидная структура. Она образуется в основном в виде комбинаций вышеназванных топологий вычислительных сетей (рис. 15.5).

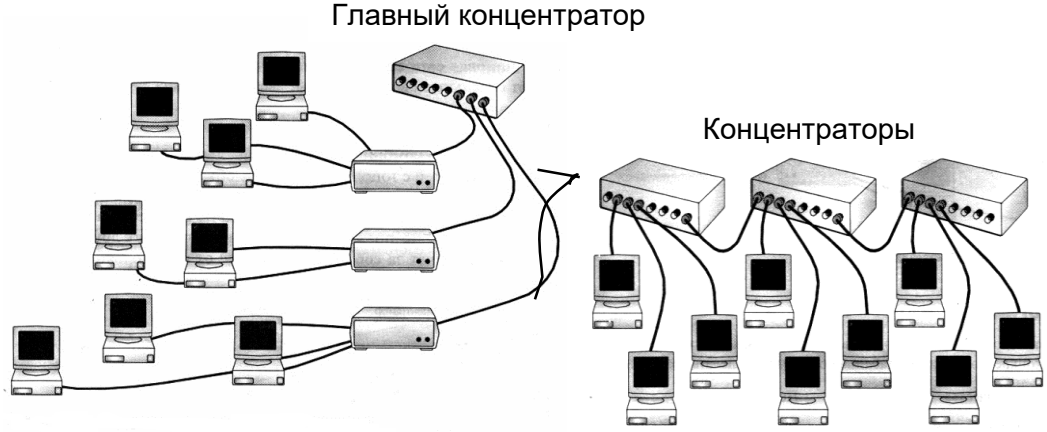


Рис. 15.5. Комбинированная топология ЛКС

Основание дерева вычислительной сети располагается в точке (корень – главный концентратор), в которой собираются коммуникационные линии информации (ветви дерева).

Вычислительные сети с древовидной структурой применяются там, где невозможно непосредственное применение базовых сетевых структур в чистом виде.

15.2. Сетевые технологии

Типичными методами доступа к передающей среде в современных ЛКС являются:

- множественный доступ с контролем несущей и обнаружением конфликтов *CSMA/CD* (метод доступа *Ethernet*);
- маркерное кольцо (метод доступа *Token Ring*);
- маркерная шина (метод доступа *Arcnet*);
- оптоволоконный интерфейс распределенных данных (технология *FDDI*).

Указанные методы реализованы соответственно стандартами *IEEE*802.3, *IEEE*802.5, *IEEE*802.4, *IEEE*802.8.

15.2.1. Технология Ethernet

Разработана в исследовательском центре компании *Xerox*. Термин *Ethernet* чаще всего используют для описания всех локальных сетей, работающих в соответствии с принципами *CSMA/CD* (*Carrier Sense MultIPle Access/Collision Detection*) – множественного доступа с контролем несущей и обнаружением коллизий, что соответствует спецификации *Ethernet IEEE* 802.3.

Протокол *CSMA/CD* состоит из двух частей: *Carrier Sense MultIPle Access* и *Collision Detection.*

Первая часть определяет, каким образом рабочая станция с сетевым адаптером «ловит» момент, когда ей следует послать сообщение. В соответствии с протоколом *CSMA* рабочая станция вначале слушает сеть, чтобы определить, не передается ли в данный момент какое-либо другое сообщение. Если слышится несущий сигнал (*carrier tone*), значит, в данный момент сеть занята другим сообщением – рабочая станция переходит в режим ожидания и находится в нем до тех пор, пока сеть не освободится. Когда в сети наступает молчание, станция начинает передачу.

Вторая часть – *Collision Detection* – служит для разрешения ситуаций, когда две или более рабочие станции пытаются передавать сообщения одновременно. Если две станции начнут передавать свои пакеты одновременно, передаваемые данные наложатся друг на друга и ни одно из сообщений не дойдет до получателя. Такую ситуацию называют *конфликтом*, или коллизией (сигналы одной станции перемешиваются с сигналами другой). *Collision Detection* требует, чтобы станция прослушала сеть также и после передачи пакета. Если обнаруживается конфликт, станция повторяет передачу пакета через случайным образом выбранный промежуток времени. Затем она вновь проверяет, не произошел ли конфликт. Термин «множественный доступ» подчеркивает тот факт, что все станции имеют одинаковое право на доступ к сети.

Если одна из станций обнаружит коллизию, она пошлет специальный сигнал, предупреждающий другие станции о произошедшем конфликте. При коллизии уничтожаются все данные в сети. После коллизии станции пытаются передать данные повторно. Этапы доступа к среде иллюстрируются рис. (15.6).

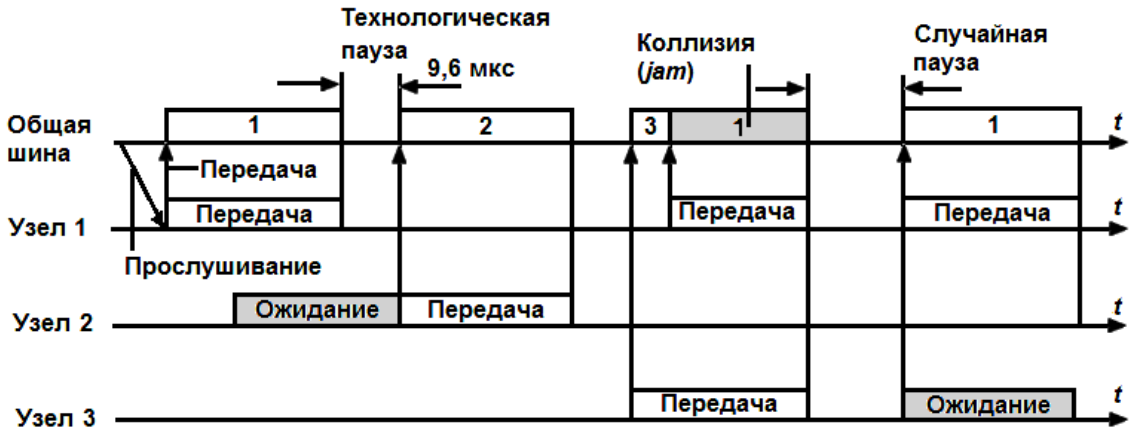


Рис. 15.6. Доступ к передающей среде при топологии *Ethernet*

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения.

Чтобы получить возможность передавать кадр, станция должна убедиться, что разделяемая их среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется

несущей частотой (*carrier-sense, CS*). Признак незанятости среды – отсутствие на ней несущей частоты, которая при манчестерском способе кодирования равна 5 – 10 МГц в зависимости от последовательности единиц и нулей, передаваемых в данный момент.

Если среда свободна, то узел имеет право начать передачу кадра. Этот кадр изображен на рисунке первым. Узел 1 обнаружил, что среда свободна, и начал передавать свой кадр. В классической сети *Ethernet* на коаксиальном кабеле сигналы передатчика узла 1 распространяются в обе стороны, так что все узлы сети их получают. Кадр данных всегда сопровождается *преамбулой (preamble),* которая состоит из 7 байт, состоящих из значений 10101010, и 8-го байта, равного 10101011. Преамбула нужна для вхождения приемника в побитовый и побайтовый синхронизм с передатчиком.

Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные, передает их вверх по своему стеку, а затем посылает по кабелю кадр-ответ. Адрес станции источника содержится в исходном кадре, поэтому станция-получатель знает, кому нужно послать ответ.

Узел 2 во время передачи кадра узлом 1 также пытался начать передачу своего кадра, однако обнаружил, что среда занята – на ней присутствует несущая частота, поэтому узел 2 вынужден ждать, пока узел 1 не прекратит передачу кадра.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу (*Inter Packet Gap*) 9,6 мкс. Эта пауза, называемая также межкадровым интервалом, нужна для приведения сетевых адаптеров в исходное состояние, а также предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна. Из-за задержек распространения сигнала по кабелю не все узлы строго одновременно фиксируют факт окончания передачи кадра узлом 1.

В приведенном примере узел 2 дождался окончания передачи кадра узлом 1, сделал паузу 9,6 мкс и начал передачу своего кадра.

Для того чтобы предотвратить одновременную передачу, был разработан специальный механизм прерываний, который предписывает каждой станции выждать случайный промежуток времени перед повторной передачей. Станция, которой достался самый короткий период ожидания, первой получит право на очередную попытку передать данные, а остальные определят, что сеть занята, и вновь будут ожидать. Единицей измерения времени ожидания является удвоенное время распространения сигнала из конца в конец отрезка кабеля, равное примерно 51,2 мс. После первого конфликта каждая станция ждет 0 или 1 единицу времени, прежде чем попытается возобновить передачу. Если снова произошел конфликт, что может быть, если две станции выбрали одно и то же число, то каждая из них выбирает одно из четырех случайных чисел: 0, 1, 2, 3. Если и в третий раз произошел конфликт, случайное число выбирается из интервала 0 – 7 и т. д. После десяти последовательных конфликтов интервал выбора случайных чисел фиксируется и становится равным 0 – 1023. После шестнадцати конфликтов контроллер отказывается от дальнейших попыток передать кадр и сообщает об этом компьютеру. Все дальнейшие действия по выходу из сложившейся ситуации осуществляются под руководством протоколов верхнего уровня. Такой алгоритм позволяет разрешить коллизии, когда конфликтующих станций немного.

Обнаружение конфликта основано на сравнении посланных сигналов и сигналов других рабочих станций. Аппаратное обеспечение станции должно во время передачи «прослушивать» кабель для определения факта коллизии. Если сигнал, который станция регистрирует, отличается от передаваемого ею, значит, произошла коллизия.

Сеть *Ethernet* относится к категории *широковещательных*. В таких сетях все станции видят все кадры вне зависимости от того, являются ли они их получателями. Каждая станция должна проверять, не ей ли предназначаются передаваемые данные. Полученные данные передаются на следующий уровень.

Основные спецификации Ethernet

Основные спецификации *Ethernet*: 10*Base*-5, 10*Base*-2, 10*Base-T*, 10*Base-F*. Каждая из разновидностей *Ethernet* предусматривает те или иные ограничения на протяженность и тип сегмента кабеля.

Стандарт 10*Base*-5 в основном соответствует экспериментальной сети *Ethernet* фирмы *Xerox* и может считаться классическим

Ethernet. Он использует в качестве среды передачи данных коаксиальный кабель с волновым сопротивлением 50 Ом, диаметром центрального медного провода 2,17 мм и внешним диаметром около 10 мм («толстый» *Ethernet*). Такими характеристиками обладают кабели марок *RG-SHRG*-11.

Различные компоненты сети, состоящей из трех сегментов, соединенных повторителями, выполненной на «толстом» коаксиале, показаны на рис. 15.7.

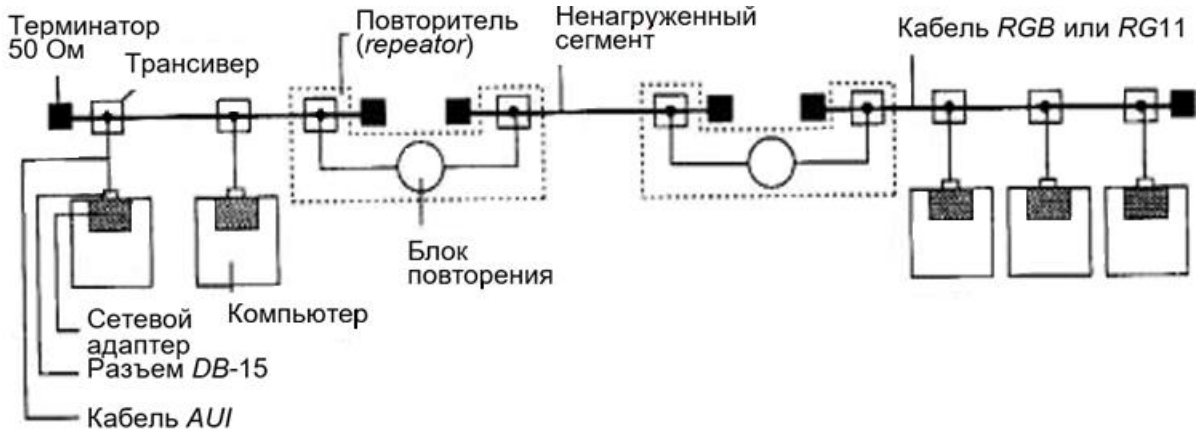


Рис. 15.7. Компоненты сети *Ethernet* на «толстом» коаксиале

Стандарт 10*Base*-2 использует в качестве передающей среды коаксиальный кабель с диаметром центрального медного провода 0,89 мм и внешним диаметром около 5 мм («тонкий» *Ethernet*). Кабель имеет волновое сопротивление 50 Ом. Такими характеристиками обладают кабели марок *RG*-58 /*U*, *RG*-58 *A/U*, *RG*-58 *C/U*.

Максимальная длина сегмента без повторителей составляет 185 м, сегмент должен иметь на концах согласующие терминаторы 50 Ом.

Типичный состав сети стандарта 10*Base*-2, состоящей из одного сегмента кабеля, показан на рис. 15.8.

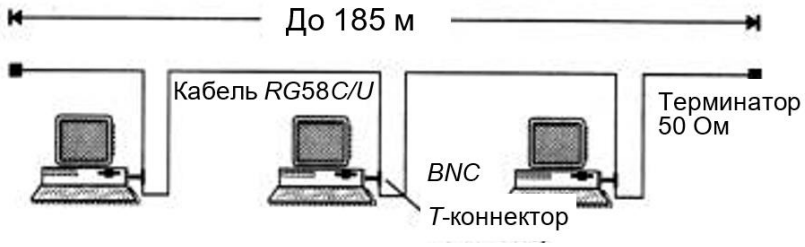


Рис. 15.8. Типичный состав сети стандарта 10*Base*-2

Сети 10*Base-T* используют в качестве среды две *неэкранированные витые пары* (*Unshielded Twisted Pair*, *UTP*).

Конечные узлы соединяются по топологии «точка-точка» со специальным устройством – многопортовым повторителем с помощью двух витых пар. Одна витая пара требуется для передачи данных от станции к повторителю (выход T_x сетевого адаптера), а другая – для передачи данных от повторителя к станции (вход R_x сетевого адаптера). На рис. 15.9 показан пример трехпортового повторителя. Повторитель принимает сигналы от одного из конечных узлов и синхронно передает их на все свои остальные порты, кроме того, с которого поступили сигналы.

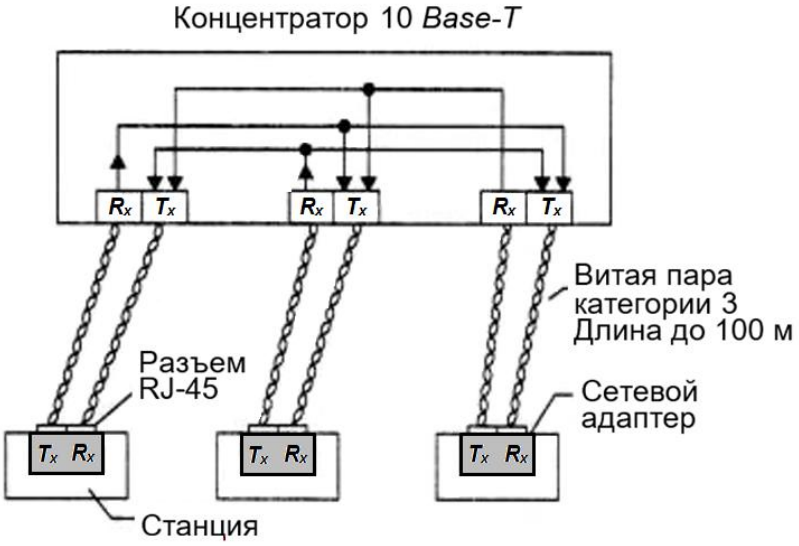


Рис. 15.9. Трехпортовый повторитель: T_x – передатчик; R_x – приемник

Для обеспечения синхронизации станций при реализации процедур доступа *CSMA/CD* и надежного распознавания станциями коллизий в стандарте определено максимально число концентраторов между любыми двумя станциями сети, а именно 4. Это правило носит название «правило 4 хабов» и оно заменяет «правило 5-4-3», применяемое к коаксиальным сетям. При создании сети 10*Base-T* с большим числом станций концентраторы можно соединять друг с другом иерархическим способом, образуя древовидную структуру (рис. 15.10).

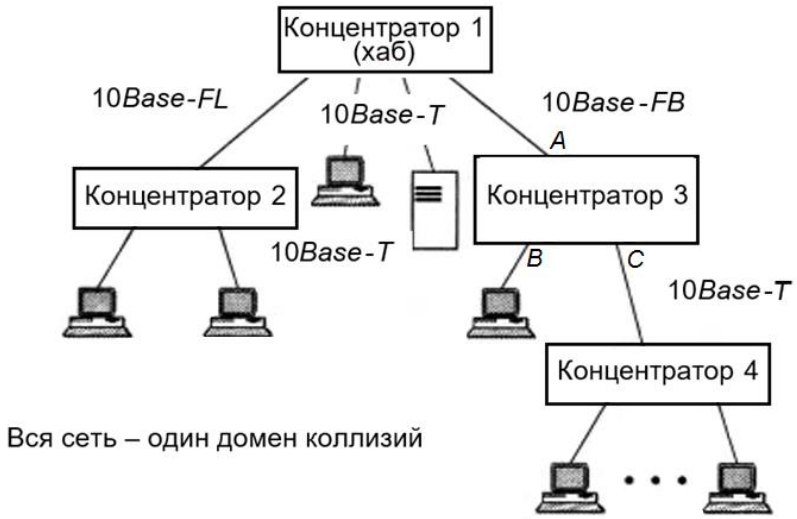


Рис. 15.10. Древовидная структура сети 10*Base-T*

Общее количество станций в сети 10*Base-T* не должно превышать общего предела в 1024, и для данного типа физического уровня этой величины действительно можно достичь.

Функционально сеть *Ethernet* на оптическом кабеле состоит из тех же элементов, что и сеть стандарта 10*Base-T* – сетевых адаптеров, многопортового повторителя и отрезков кабеля, соединяющих адаптер с портом повторителя. Как и в случае витой пары, для соединения адаптера с повторителем используются два оптоволокна – одно соединяет выход T_x адаптера со входом R_x повторителя, а другое – вход R_x адаптера с выходом T_x повторителя.

Оптоволоконные стандарты 10Base-F (*FB, FL*) гарантируют длину оптоволоконной связи между повторителями до 2 км при общей длине сети не более 2500 м. Максимальное число повторителей между любыми узлами сети – 5.

Теоретическая производительность сети *Ethernet* составляет 10 Мб/с. Однако нужно учитывать, что из-за коллизий технология *Ethernet* никогда не сможет достичь своей максимальной производительности, реальная производительность *Ethernet* не превышает 70 % от теоретической.

Данные, передаваемые в сети *Ethernet*, разбиты на *кадры*. Для успешной доставки информации получателю каждый кадр должен кроме данных содержать дополнительную служебную информацию: длину поля данных, физические адреса отправителя и получателя, тип сетевого протокола и т.д.

Для того чтобы рабочие станции имели возможность взаимодействовать с сервером в одном сегменте сети, они должны поддерживать единый формат кадра. Существуют четыре основные разновидности кадров *Ethernet*:

- *Ethernet Type* II,
- *Ethernet* 802.3,
- *Ethernet* 802.2,
- *Ethernet SNAP* (*SubNetwork Access Protocol*).

Общие для всех четырех типов кадров являются поля: преамбула, признак начала кадра (1), адрес получателя (2), адрес отправителя (3), длина/тип (4), данные (5) и контрольная сумма (6).

Минимальная допустимая длина кадров *Ethernet* составляет 64 байта, а максимальная – 1518 байт. Так как на служебную информацию в кадре отводится 18 байт, то поле «Данные» может иметь длину от 46 до 1500 байт. Если передаваемые по сети данные меньше допустимой минимальной длины, кадр будет автоматически дополняться до 46 байт. Столь жесткие ограничения на минимальную длину кадра введены для обеспечения нормальной работы механизма обнаружения коллизий.

В начале 1990-х гг. начала ощущаться недостаточная пропускная способность *Ethernet*. Многие сегменты *Ethernet* на 10 Мб/с стали перегруженными, время реакции серверов и частота возникновения коллизий в таких сегментах значительно возросли, еще более снижая реальную пропускную способность. В ответ на эти требования была разработана технология *Fast Ethernet*, являющаяся 100-мегабитной версией *Ethernet*.

15.2.2. Fast Ethernet

Стандарт *Fast Ethernet* определяет три модификации для работы с разными видами кабелей: 100*BaseTX*, 100*BaseT*4 и 100*BaseFX*. Модификации 100*BaseTX* и 100*BaseT*4 рассчитаны на витую пару, а 100*BaseFX* был разработан для оптического кабеля.

Преемственность технологий *Fast Ethernet* и *Ethernet* позволяет легко выработать рекомендации по применению: *Fast Ethernet* целесообразно применять в тех организациях, которые широко использовали

классический *Ethernet*, но сегодня испытывают потребность в увеличении пропускной способности. При этом сохраняются весь накопленный опыт работы с *Ethernet* и частично сетевая инфраструктура.

Хотя *Fast Ethernet* и является развитием стандарта *Ethernet*, переход к 100*BaseT* требует некоторого изменения в топологии сети. Теоретический предел диаметра сегмента сети *Fast Ethernet* составляет 250 м. Это ограничение определено самой природой метода доступа *CSMA/CD* и скоростью передачи 100 Мб/с.

Для классического *Ethernet* время прослушивания сети определяется максимальным расстоянием, которое 512-битный кадр может пройти по сети за время, равное времени обработки этого кадра на рабочей станции. Для сети *Ethernet* это расстояние равно 2500 м. В сети *Fast Ethernet* этот же самый 512-битный кадр за время, необходимое на его обработку на рабочей станции, пройдет всего 250 м. Если принимающая станция будет удалена от передающей на расстояние свыше 250 м, то кадр может вступить в конфликт с другим кадром на линии, а передающая станция, завершив передачу, уже опоздала бы с реакцией на этот конфликт. Поэтому максимальный диаметр сети 100*BaseT* составляет 250 м.

Для увеличения допустимой дистанции необходимо использовать повторители для соединения узлов. Основная область использования *Fast Ethernet* сегодня – это сети рабочих групп и отделов. Целесообразно совершать переход к *Fast Ethernet* постепенно, оставляя *Ethernet* там, где он хорошо справляется с поставленными задачами.

15.2.3. Стандарт Gigabit Ethernet

Технология *Gigabit Ethernet* разработана в ноябре 1995 г., когда была сформирована рабочая группа (*IEEE* 802.3z), рассматривающая возможность развития *Fast Ethernet* до гигабитных скоростей. Она представляет собой дальнейшее развитие стандартов 802.3 для сетей *Ethernet* с пропускной способностью 10 и 100 Мб/с.

В основном продукты, поддерживающие технологию *Gigabit Ethernet*, планируется внедрять в центре корпоративной сети. Наиболее быстрый и простой путь получения отдачи от внедрения *Gigabit*

Ethernet состоит в замене традиционных коммутаторов *Fast Ethernet* на концентраторы или коммутаторы *Gigabit Ethernet*.

К недостаткам технологии *Gigabit Ethernet* можно отнести отсутствие встроенного механизма поддержки качества обслуживания.

Самый простой способ получения немедленной выгоды от использования новой технологии – организация на ее основе магистрали сети с последующим подключением серверов. Кроме установки новых коммутаторов и сетевых адаптеров, никаких изменений не потребуется.

15.2.4. Технология Token Ring

Сети *Token Ring* так же, как и сети *Ethernet*, характеризует разделяемая среда передачи данных, которая в данном случае состоит из отрезков кабеля, соединяющих все станции сети в кольцо. 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)*.

Технология *Token Ring* была разработана компанией IBM в 1984 г., а затем передана в качестве проекта стандарта в комитет *IEEE* 802, который на ее основе принял в 1985 г. стандарт 802.5. Компания *IBM* использует технологию *Token Ring* в качестве своей основной сетевой технологии для построения локальных сетей на основе компьютеров различных классов – мэйнфреймов, мини-компьютеров и персональных компьютеров. В настоящее время именно компания IBM основной законодатель моды технологии *Token Ring*, производящий около 60 % сетевых адаптеров этой технологии.

Сети *Token Ring* работают с двумя битовыми скоростями – 4 и 16 Мб/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается. Сети *Token Ring*, работающие со скоростью 16 Мб/с, имеют некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мб/с.

В сети *Token Ring* определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры – посланный кадр всегда возвращается в станцию-отправитель (рис. 15.11).

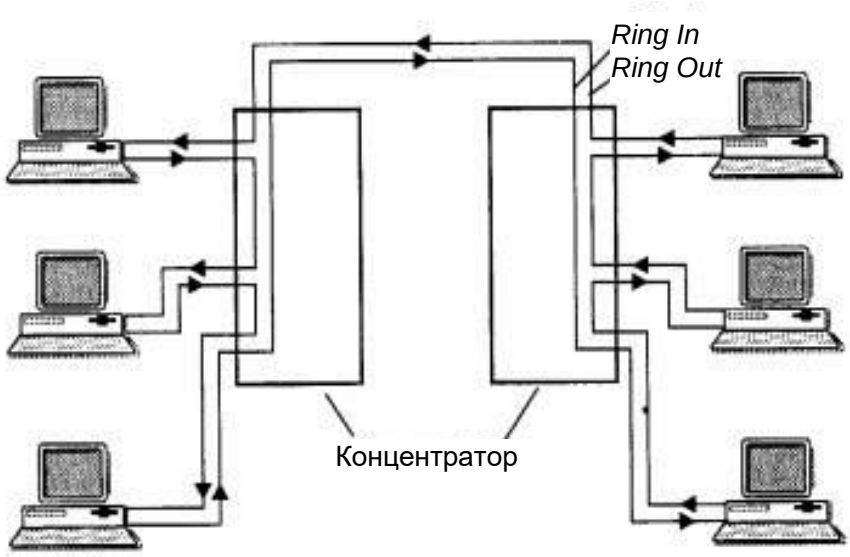


Рис. 15.11. Сеть *Token Ring*

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.

Стандарт *Token Ring* фирмы *IBM* изначально предусматривал построение связей в сети с помощью концентраторов, называемых *MSAU* (*Multi-Station Access Unit*), то есть устройствами многостанционного доступа. Сеть *Token Ring* может включать до 260 узлов.

15.2.5. Технология ARCnet

Технология *Attached Resourse Computing Network* (*ARCnet*) – сетевая архитектура, разработана компанией *Datapoint* в середине 1970-х гг. Это селективный метод доступа в моноканал, называемый «маркерная шина».

В качестве стандарта *IEEE ARCnet* принят не был, но частично соответствует *IEEE* 802.4. Это сеть с передачей маркера, топология – «звезда» или «шина». В качестве среды передачи *ARCnet* может использовать коаксиальный кабель, витую пару и оптоволоконный кабель.

Закрепить свои позиции этому недорогому стандарту помешало малое быстродействие – всего 2,5 Мб/с. В начале 90-х гг. *Datapoint* разработала *ARCNETPLUS*, со скоростью передачи до 20 Мб/с, обратно совместимый с *ARCnet*. Но время было упущено – чересчур медленный *ARCnet* к тому времени мало где выжил, а «в спину новому *ARCNETPLUS* уже дышал *Fast Ethernet*». Но есть место для применения *ARCnet* и в современной сети. Допустимая длина коаксиального кабеля при топологии «звезда» – 610 м. Это дешевый и неплохой вариант для соединения локальных сетей в двух рядом стоящих зданиях.

15.2.6. 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.

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*. Узлы, которые хотят сделать самыми надежными, должны быть подключены к обоим кольцам (рис. 15.12).

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 (рис. 15.13).

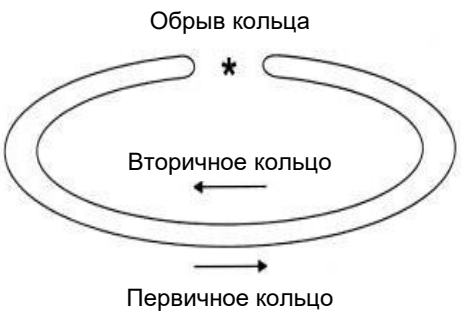


Рис. 15.12. Сеть *FDDI*

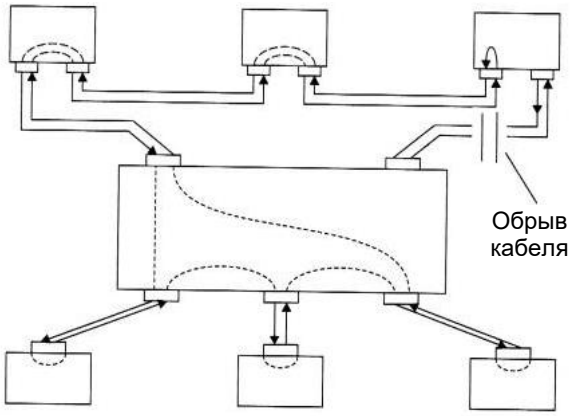


Рис. 15.13. Нормальный режим работы сети *FDDI*

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется со вторичным, вновь образуя единое кольцо (рис. 15.14).

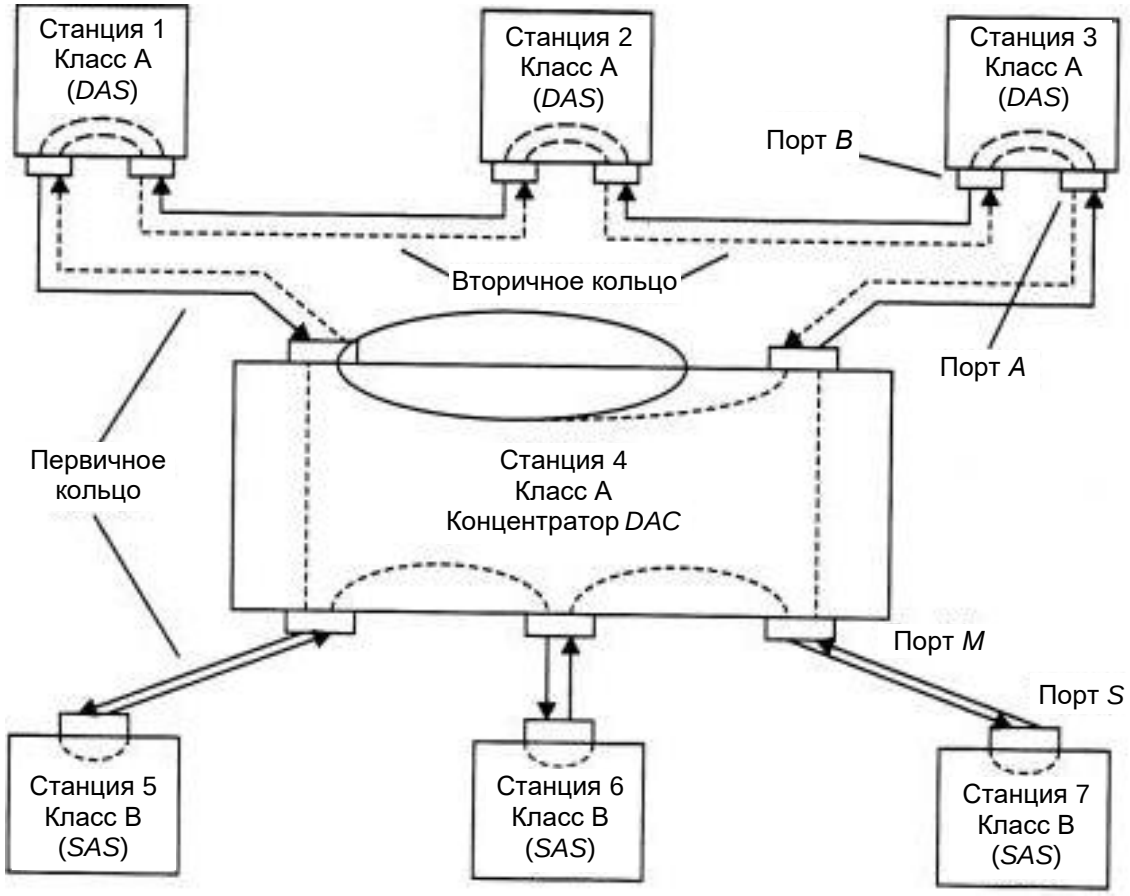


Рис. 15.14. Режим работы сети *FDDI* в случае отказа

Этот режим работы сети называется *Wrap*, то есть «свертывание», или «сворачивание» колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров *FDDI*. Для упрощения этой процедуры данные по первичному 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.

15.2.7. Домашние сети на базе электропроводки

Эта технология появилась совсем недавно и получила название *HomePLC* (*PowerLine Communication*), или просто «*HomePlug*». Технология *PLC* основана на использовании силовых электросетей для информационного обмена, предлагает следующее решение данной проблемы. С одной стороны, питающие здание электрические кабели служат «последней милей» для передачи данных. С другой стороны, электропроводка внутри здания играет роль «последнего дюйма». Разделение между внешней (наружной) системой (*Outdoor*) и внутренней (*Indoor*) позволяет им обеим работать одновременно и независимо друг от друга, используя одну и ту же передающую среду и различные несущие частоты.

Основа технологии *PowerLine* – использование частотного разделения сигнала, при котором высокоскоростной поток данных разбирается на несколько относительно низкоскоростных потоков, каждый из которых передается на отдельной поднесущей частоте (*Freq*1 – *Freq*4) с последующим их объединением в один сигнал (рис. 15.15). Реально в технологии *PowerLine* используются 84 поднесущие частоты в диапазоне 4 – 21 МГц.

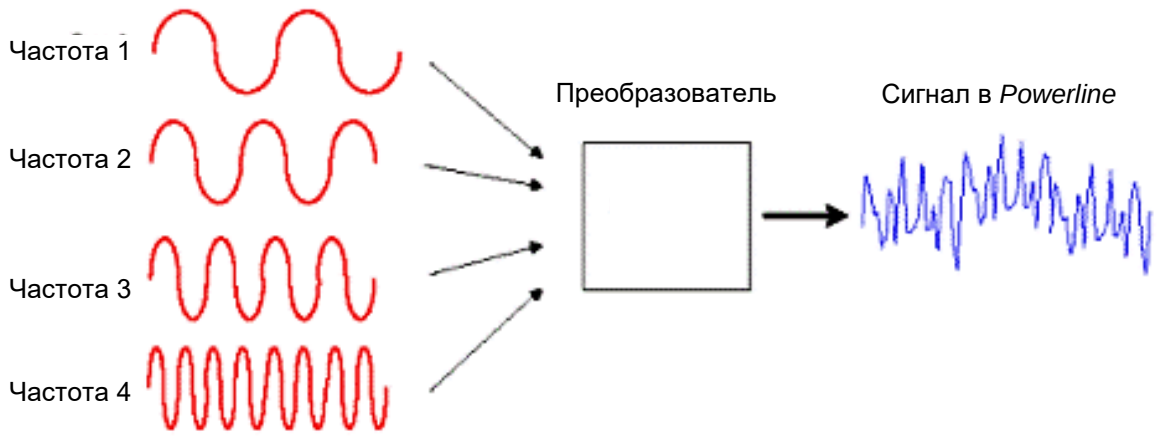


Рис. 15.15. Частотное разделение

На рис. 15.16 изображен пример небольшой домашней сети, состоящей из трех компьютеров, использующей технологию *Powerline* с выходом в *Internet*.

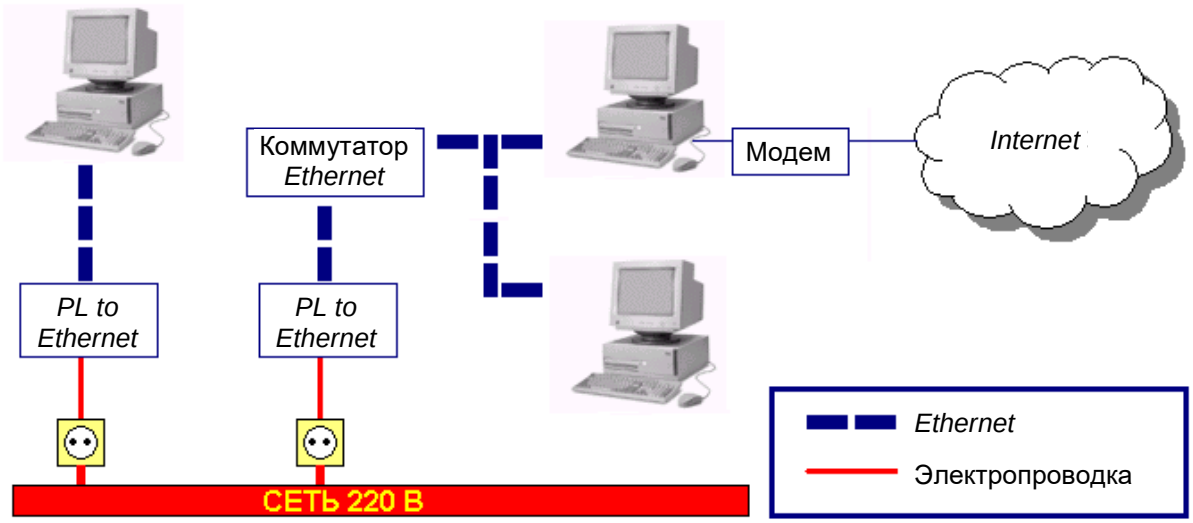


Рис. 15.16. Пример небольшой сети с использованием технологии *Powerline*

Один из компьютеров подключается непосредственно к среде передачи данных, то есть к электропроводке, используя адаптер *Powerline to Ethernet*. На данном компьютере должен быть установлен *Internet*-адаптер. Другие два компьютера подключены в домашнюю сеть через обыкновенный *Internet*-коммутатор (*switch*), который, в свою очередь, подключается к электросети с помощью адаптера *Powerline to Ethernet*. Далее к одному из компьютеров подключен модем. Если правильно настроить программное обеспечение, этот компьютер будет выступать в роли *Internet*-шлюза и все компьютеры получать доступ к *Internet*.

Преимущества *PLC*-технологии в сравнении с существующими технологиями передачи данных заключаются в следующем:

- не требует наличия сети кабельного телевидения или телефонной сети и, следовательно, дорогостоящих работ, связанных с прокладкой дополнительного кабеля;
- очень быстрое развертывание и возможность поэтапного наращивания по мере необходимости;
- обеспечивает предоставление услуг практически во всех местах, где есть электропроводка;

• предполагает низкие начальные капиталовложения;

• обеспечивает возможность предоставления не только высокоскоростного доступа в *Internet*, но и телефонной связи (локальной, с выходом в городские телефонные сети);

• дает возможность предоставления энергетических услуг и услуг по управлению «интеллектуальным домом» (автоматическое снятие показаний различных счетчиков, дистанционный мониторинг, сигнализация и др.);

• возможность комплексного предоставления энергетических и телекоммуникационных услуг одним поставщиком.

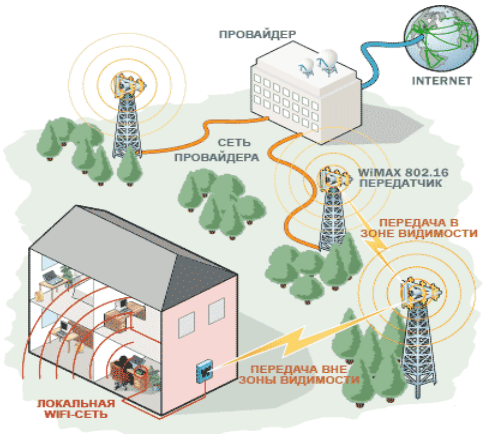
В настоящее время на базе оборудования *Ascom Powerline Communications AG* уже реализованы ряд инновационных проектов по использованию технологии передачи информации в странах Восточной Европы. Конечно же, больше всего успешных проектов по организации широкополосного доступа через электросети реализовано в США – на родине *Internet*. Известны такие компании, как *New Visions* (Нью-Йорк), *Communications Technologies* (штат Виргиния), *Cinergy* (штат Огайо). В Германии *PLC* предлагают *Vype; PIPer-Net* и *PowerKom*; в Австрии – *Speed-Web*; в Швеции – *ENkom*; в Нидерландах – *Digistroom*; в Шотландии – *Broadband*. В 2005 г. и в Российской Федерации началось развертывание сетей доступа в *Internet* через бытовые электрические сети по технологии *PLC*. Таким образом, практическая реализация подтверждает уникальность и целесообразность применения высокоэффективной технологии *PLC* в сфере телекоммуникаций.

Попытки ряда крупных компаний, объединившихся под эгидой некоммерческой организации *HomePlug Powerline Alliance*, продвигать этот стандарт в качестве способа создания домашних сетей, в том числе с подключением к *Internet*, пока особым успехом не увенчались. Однако сетевое оборудование *HomePlug* имеется в продаже. Большинство из таких устройств на практике – *конвертеры* (преобразователи), обеспечивающие подключение к сети *HomePlug* адаптеров таких популярных сетевых технологий, как *Ethernet* или *Wi-Fi*.

Вопросы к компьютерному тестированию

1. На основе каких стандартов сетей были созданы стандарты *ISO* 8802-1...5?
2. Какой стандарт разработан американским институтом по стандартизации *ANSI*?
3. В какой топологии в случае выхода из строя хотя бы одной из рабочих станций вся сеть парализуется?
4. Что увеличивается пропорционально количеству рабочих станций, входящих в вычислительную сеть при кольцевой топологии?
5. Как называется уровень, обеспечивающий корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети?
6. Как называется топология компьютерной сети, при которой среда передачи информации представляется в форме коммуникационного пути, доступного для всех рабочих станций, к которому они все должны быть подключены?
7. Что является особенностью использования сетей с топологией типа «звезда»?
8. При какой из топологий сети существуют ограничения на протяженность вычислительной сети, и в случае выхода из строя хотя бы одной из рабочих станций вся сеть парализуется?
9. Как называется топология, в которой основание вычислительной сети располагается в точке, где собираются коммуникационные линии информации?
10. Как называется метод доступа к передающей среде, представляющий множественный доступ с контролем несущей и обнаружением конфликтов?
11. На что введены ограничения во всех разновидностях *Ethernet*?
12. В соответствии с каким протоколом (привести аббревиатуру) работает технология *Ethernet*?
13. Какая из частей протокола *Carrier Sense MultIPle Access/Collision Detection* технологии *Ethernet* служит для разрешения коллизий?

14. Что является признаком незанятости линии передачи данных при использовании протокола *CSMA/CD* технологии *Ethernet*?
15. В каком из стандартов максимальное число концентраторов между любыми двумя станциями сети равно 4?
16. Вставьте пропущенное слово: При создании сети 10*Base-T* с большим числом станций концентраторы можно соединять друг с другом, образовав _____ структуру.
17. Какой стандарт определяет три модификации для работы с разными видами кабелей: 100*Base-TX*, 100*Base-T*4, 100*Base-FX*?
18. Какой теоретический предел диаметра сегмента сети *Fast Ethernet*?
19. Какие сети характеризует разделяемая среда передачи данных, состоящая из отрезков кабеля, соединяющих все станции сети в кольцо?
20. Какая спецификация *Ethernet* предусматривает использование тонкого коаксиального кабеля («тонкий» *Ethernet*)?
21. Каково максимальное число повторителей в сети с оптоволоконным стандартом 10*Base-F* (*FB, FL*)?
22. Назовите первую технологию локальных сетей, в которой средой передачи данных является волоконно-оптический кабель.
23. Какова среда передачи данных у технологии *Token Ring*?
24. В какой топологии выполняют сети *FDDI*?
25. Что может использовать в качестве среды передачи технология *ARCnet*?
26. Какая из технологий строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети?
27. В каком направлении в технологии *FDDI* передаются данные по первичному кольцу?
28. Какой диапазон поднесущей частоты используется в технологии *PowerLine* (МГц)?
29. Какие сетевые устройства используются технологией *PowerLine* для подключения к силовой электросети?



Глава 16

БЕСПРОВОДНЫЕ ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Рассматриваемые вопросы:

16.1. Технология *Bluetooth*.
16.2. Технология *GPRS*.
16.3. Беспроводная передача данных по технологии *Wi-Fi*.
16.4. Технология *MIMO*.
16.5. Технология *Mesh*.
16.6. Технология *WiMAX*.

Сеть *WLAN* (*Wireless Local Area Network* – беспроводная локальная сеть), использующая для связи и передачи данных между узлами вместо кабельных соединений инфракрасный световой или высокочастотный радиосигнал. Это гибкая система передачи данных, применяемая внутри одного офиса, здания или в пределах определенной территории.

Стандартный ИК-интерфейс способен передавать информацию со скоростью 115,2 кб/с, а с учетом существующего расширения, предложенного компаниями *IBM Hewlett-Packard* и *Sharp*, – до 4 Мб/с.

В 1994 г. был разработан *IrDA-Standart IEEE* 802.11, являющийся основой для всех последующих разработок стандартов беспроводных сетей.

Сеть высокочастотного радиосигнала использует беспроводные адаптеры, содержащие передатчики и приемники, которые заменяют проводные соединения. Существует ряд технологий таких сетей.

16.1. Технология *Bluetooth*

Дословно «*Bluetooth*» переводится на русский как «Синий зуб». Устройства, образующие между собой *Bluetooth*-соединение, образуют сеть, называемую *пикосеть (piconet)*. В ней одно устройство – *главное (master)*, а другое – *подчиненное (slave)*. К одному *master*-устройству

может быть подключено несколько *slave*-устройств. Пикосети могут объединяться, образуя *скеттерсеть (scatternet)*. В этом случае соединяются два главных устройства, одно из которых становится *главным/подчиненным*. Возможные топологии пикосетей показаны на рис. 16.1

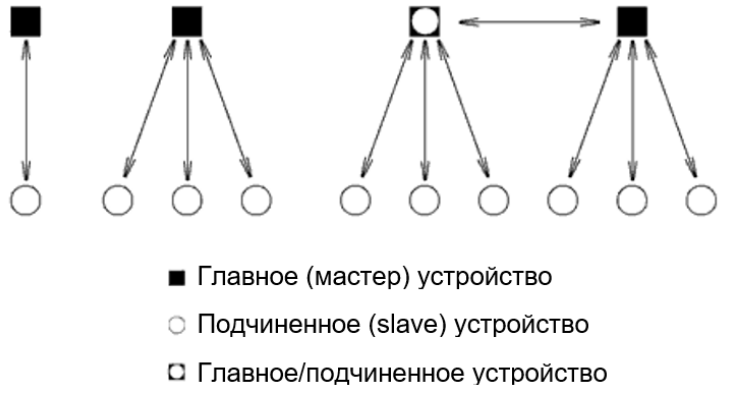


Рис. 16.1. Возможные топологии пикосетей

Интерфейс *Bluetooth* состоит из трех частей: *приемопередатчик*, *контроллер связи* и *управляющее устройство*, осуществляющее связь с терминалом. Терминалом может быть любой прибор, будь то мобильный телефон, планшет или ноутбук. Приемопередатчик и контроллер связи, как правило, выполнены на отдельных микросхемах, а вот функции управляющего устройства может выполнять и процессор терминала при достаточной собственной мощности. Блок-схема организации *Bluetooth*-связи показана на рис. 16.2.

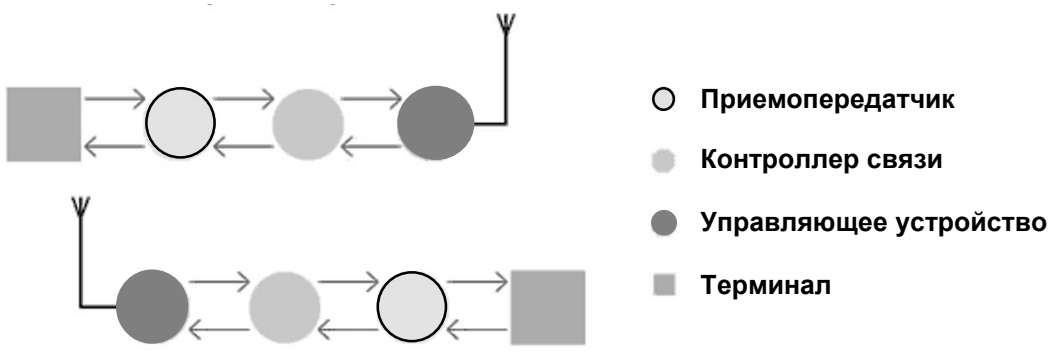


Рис. 16.2. Блок-схема организации *Bluetooth*-связи

Схема проста в реализации как в аппаратном, так и в программном направлении, что сказывается на популярности интерфейса *Bluetooth*.

Версии Bluetooth и их характеристики

• *Bluetooth 1.0* – самая первая версия интерфейса, не была стандартизована, поэтому устройства, поддерживающие данный интерфейс, не всегда могли беспрепятственно «состыковаться».

• *Bluetooth v1.1* – несла в себе исправления многих ошибок предыдущей версии, а также была способна на передачу информации по нешифрованным каналам и индикацию уровня мощности сигнала.

• *Bluetooth 1.2* – появилась в первой половине 2003 г., обеспечивает передачу информации со скоростью 2 – 3 Мб/с.

• *Bluetooth 2.0* – скорость увеличена до 12 Мб/с.

Протоколы Bluetooth

• *Basehand (базовая полоса)*. Осуществляет физическое соединение между двумя и более устройствами. Возможны два типа соединения: *SCO (синхронное)* и *ACL (асинхронное)*. По *SCO* можно передавать данные или данные с аудиопотоком, например голосом. По *ACL* передается только аудиопоток.

• *TCS BIN (TCS Binary* – контроль телефонии**)**. Иными словами, двоичный протокол управления телефонией. Выполняет контроль сигнализации вызова для установления речевого вызова и вызова данных между устройствами *Bluetooth*.

• *PPP (Point-to-Point Protocol* – «Точка-точка»**)**. Служит для передачи *IP*-пакетов с уровня *PPP* на уровень локальных сетей.

• *TCP/UDP/IP* применяется для обмена данными (в качестве моста) между протоколом *TCP*/*IP* и *Bluetooth*.

Связь *Bluetooth* применяется прежде всего для передачи информации между различными портативными устройствами, например, мобильными телефонами и планшетами, а также для обмена данными между гаджетами и настольным компьютером. Технология *Bluetooth* обеспечивает скорость передачи информации до 723 кб/с (спецификация версии 1.2) или до 2,1 Мб/с (спецификация версии 2.0) в радиусе от 10 до 100 м.

16.2. Технология *GPRS*

Технология GPRS (*General Packet Radio Service* – «пакетная радиосвязь общего пользования») – надстройка над технологией мобильной связи *GSM*, осуществляющая пакетную передачу данных и обеспе-

чивающая полноценный доступ в *Internet* по сетям сотовой связи. При этом мобильный телефон подключается к компьютеру (обычно – к ноутбуку или КПК) при помощи кабеля через порт *USB* (реже – через порт *COM*) либо беспроводным способом (при помощи *Bluetooth* или инфракрасной связи) и фактически выполняет роль модема, работающего со скоростью до 170 кб/с (рис. 16.3). Современные же модели сотовых телефонов и «смартфоны» (устройства, сочетающие в себе функции мобильного телефона и карманного компьютера) позволяют работать с *Internet* через *GPRS* при помощи встроенного программного обеспечения (программ для обмена электронной почтой, браузеров и пр.).

Рис. 16.3. Связь по технологии *GPRS*

GPRS по принципу работы аналогична *Internet*: данные разбиваются на пакеты и отправляются получателю (необязательно одним и тем же маршрутом), где происходит их сборка. При установлении сессии каждому устройству присваивается уникальный адрес, что по сути превращает его в сервер. Протокол *GPRS* прозрачен для *TCP*/*IP*, поэтому интеграция *GPRS* с *Internet* незаметна конечному пользователю. Пакеты могут иметь формат *IP* или *X*.25, при этом не имеет значения, какие протоколы используются поверх *IP*, поэтому есть возможность использования любых стандартных протоколов транспортного и прикладного уровней, применяемых в *Internet* (*TCP*, *UDP*, *HTTP*, *HTTPS*, *SSL*, *POP3*, *XMPP* и др.). Также при использовании *GPRS* мобильный телефон выступает как клиент внешней сети, и ему присваивается *IP*-адрес (постоянный или динамический).

16.3. Беспроводная передача данных по технологии *Wi-Fi*

Технологией *Wi-Fi* (*Wireless Fidelity*) – в переводе с английского – «беспроводная свобода» – называют один из форматов передачи цифровых данных по радиоканалам. Изначально устройства *Wi-Fi* были предназначены для корпоративных пользователей, чтобы заменить традиционные кабельные сети.

Данная технология предполагает наличие точки доступа/маршрутизатора *Wi-Fi* (стандарты 802.11*a/b/g/n*), которая обеспечивает стабильный доступ к сети из некоторой области радиусом до 45 м в помещении и 90 м на открытом пространстве.

Точки доступа – это специальные приемопередающие устройства, соединяющие беспроводные устройства с проводной частью общей сети и выступающие в качестве моста или маршрутизатора. На первом этапе развития архитектур беспроводных ЛВС использовались так называемые «толстые» точки доступа, однако такие ЛВС характеризовались плохой масштабируемостью и управляемостью. Современная беспроводная ЛВС – это распределенная структура с «тонкими» точками доступа и централизованным контролем и управлением (рис. 16.4).

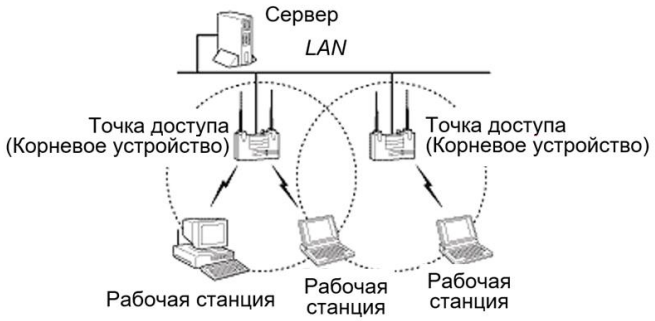


Рис. 16.4. Структура сети по технологии *Wi-Fi*

В каждом помещении устанавливаются точки доступа – их число зависит от размера помещения, числа пользователей и создаваемой ими нагрузки. Схема функционирования сети *Wi-Fi* изображена на рис. 16.5.

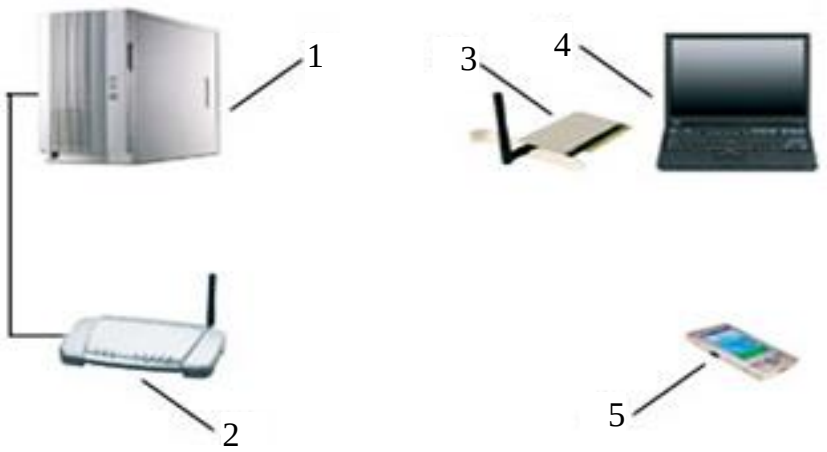


Рис. 16.5. Схема функционирования *Wi-Fi* сети:
1 – сервер; 2 – точка доступа; 3 – *Wi-Fi*-адаптер;
4, 5 – устройства локальной сети

Wi-Fi предназначен для объединения между собой двух и более устройств. Такое объединение может осуществляться тремя способами.

Объединение № 1. Одно устройство соединяется с другим устройством напрямую. Такое подключение называется «Точка-точка». В результате образуется беспроводная локальная сеть, состоящая из двух устройств, оснащенных *Wi-Fi*-адаптерами. Этими устройствами могут быть любые электронные аппараты, будь то настольные ПК, ноутбуки, планшеты, смартфоны и т.п. При соединении типа «Точка-точка» достаточно двух (по одному для каждого устройства) *Wi-Fi*-адаптеров. Они могут быть выполнены в виде *PCI*-карт расширения, а также *PCMCIA, flash*-карт и др.

Объединение № 2. Соединение более двух устройств в беспроводную локальную сеть. Все аналогично предыдущему способу, но одних только *Wi-Fi*-адаптеров в данном случае будет недостаточно. Необходима также *точка доступа Access Poin* (*AP*). *AP* соединяется проводным способом с кабелем *Internet*-соединения (если планируется выход в сеть из «воздушной» локальной сети), а беспроводным – с устройствами, оснащенными *Wi-Fi*-адаптерами.

Объединение № 3. Соединение посредством беспроводной сети Wi-Fi двух и более проводных или воздушных сетей. Выполняется данная задача при помощи все той же *AP*.

За совместимостью продуктов различных производителей *Wi-Fi* следит группа *Wi-Fi Alliance*, бывшая *WECA*, в которую входят более 80 наиболее крупнейших компаний, такие как *Cisco, Lucent, 3Com, IBM, Intel, Apple, Compaq, Dell, Fujitsu, Siemens, Sony, AMD* и пр.

Для передачи данных *Wi-Fi* использует частоты 2,4 и 5 ГГц. На сегодняшний день стандартами являются 802.11a, 802.11b и 802.11g. Связь обеспечивается в радиусе 80 – 300 м от стандартной точки доступа на открытой местности со скоростью до 54 Мб/с. При наличии более мощных антенн или усилителей сигнала передача данных может осуществляться на расстояние до 20 км.

Недостатки технологии

• Чувствительность к помехам, таким как, например, электромагнитные, излучаемые различной техникой, стоящей в зоне покрытия сети. Они влияют прежде всего на скорость соединения. Она может существенно упасть при попадании радиопотока в зону помех.

• Скорость кабельного соединения все равно остается выше, чем скорость беспроводного. По крайней мере, на равных расстояниях между источником сигнала и потребителем сигнала.

Изначально сети *Wi-Fi* из-за дорогого оборудования применялись преимущественно внутри больших корпораций, однако в настоящее время беспроводные точки доступа используются в торговых центрах, аэропортах, вокзалах, гостиницах и других оживленных местах во всех крупных городах мира.

16.4. Технология *MIMO*

Дальнейшее повышение пропускной способности и дальности действия беспроводных ЛВС обеспечивает стандарт *IEEE* 802.11*n*. Он основан на *технологии MIMO* (*MultIPle Input, MultIPle Output*), которая предусматривает передачу радиосигнала по нескольким параллельным путям между точкой доступа и клиентским устройством. При этом для каждого передаваемого потока используется отдельная пара антенн, расположенных на обоих концах канала. Благодаря технологии *MIMO* пропускная способность беспроводных ЛВС достигает отметки в 100 Мб/с, что соответствует скорости наиболее распространенного сегодня проводного варианта *Ethernet*.

Технология *MIMO* ускоряет беспроводную передачу данных за счет так называемого многолучевого распространения, которое используется для передачи большего объема данных по радиоканалу. Средствами *MIMO* по радиоканалу на 54 Мб/с можно вести передачу с фактической скоростью 108 Мб/с. На рис. 16.6 показана схема, поясняющая суть технологии.

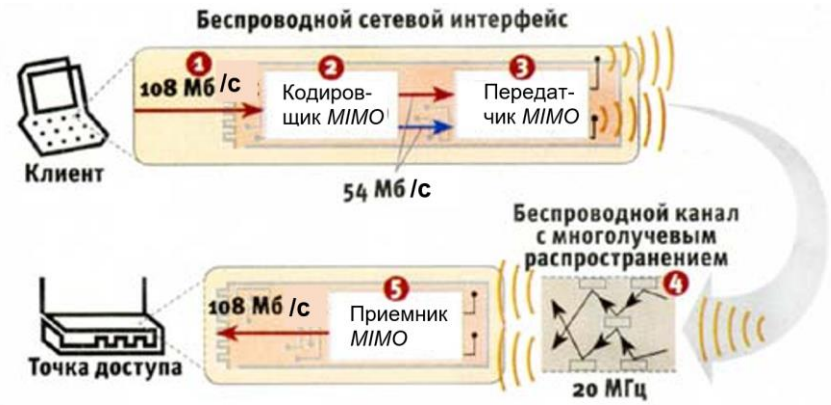


Рис. 16.6. Сеть по технологии *MIMO*

Алгоритм передачи состоит в следующем:

1. Клиент посылает данные в беспроводную сеть со скоростью 108 Мб/с.

2. Кодировщик разделяет поток данных на два или более потоков, обладающих меньшей скоростью, в данном случае – 54 Мб/с.

3. Передатчик передает каждый поток на независимую антенну, причем антенны настроены на один и тот же канал.

4. Сигналы отражаются от объектов, в результате чего создается эффект многолучевого распространения. В пределах одного радиоканала *MIMO* преобразует эти потоки в «виртуальные каналы», которые становятся носителями потоков данных.

5. Две или больше принимающие антенны воспринимают сигнал. Специальные алгоритмы приводят поток данных к исходному, сигнал восстанавливается и воспроизводится со скоростью 108 Мб/с.

16.5. Технология *Mesh*

Топология *Mesh* (пространство, или промежуток, между нитями сети) основана на децентрализованной схеме организации сети в отличие от типовых сетей 802.11*a/b/g*, которые создаются по централизованному принципу. Точки доступа, работающие в сетях *Mesh*, не только предоставляют услуги абонентского доступа, но и выполняют функции маршрутизаторов/ретрансляторов для других точек доступа той же сети. Благодаря этому появляется возможность создания самоустанавливающегося и самовосстанавливающегося сегмента широкополосной сети.

Сети *Mesh* строятся как совокупность кластеров. Территория покрытия разделяется на кластерные зоны, число которых теоретически не ограничено. В одном кластере размещаются от 8 до 16 точек доступа. Одна из таких точек является узловой (*gateway*) и подключается к магистральному информационному каналу с помощью кабеля (оптического либо электрического) или по радиоканалу (с использованием систем широкополосного доступа) (рис. 16.7).

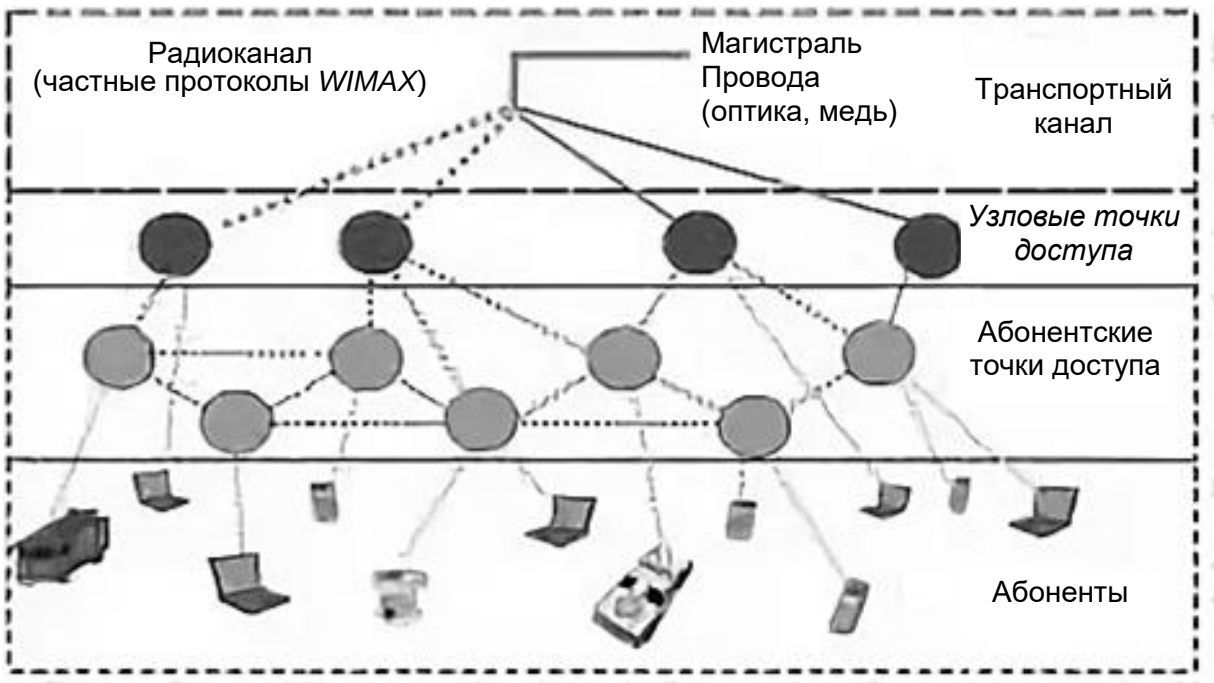


Рис. 16.7. Организация сети *Mesh*

Узловые точки доступа так же, как и остальные точки доступа (*nodes*) в кластере соединяются между собой (с ближайшими соседями) по транспортному радиоканалу. В зависимости от конкретного решения точки доступа могут выполнять функции ретранслятора (транспортный канал) либо функции ретранслятора и абонентской точки доступа. Особенностью *Mesh* является использование специальных протоколов, позволяющих каждой точке доступа создавать таблицы абонентов сети с контролем состояния транспортного канала и поддержкой динамической маршрутизации трафика по оптимальному маршруту между соседними точками.

При отказе какой-либо из них происходит автоматическое перенаправление трафика по другому маршруту, что гарантирует не просто доставку трафика адресату, а доставку за минимальное время.

Процедура расширения сети в пределах кластера ограничивается установкой новых точек доступа, интеграция которых в существующую сеть происходит автоматически.

Недостаток подобных сетей заключается в том, что они используют промежуточные пункты для передачи данных; это может вызвать задержку при пересылке информации и как следствие снизить качество трафика реального времени (например, речи или видео), поэтому существуют ограничения на количество точек доступа в одном кластере.

Основной стандарт технологии – *IEEE* 802.11*s*, описывающий ее основные функции и позволяющий беспроводным узлам обнаруживать друг друга, устанавливать связь и вырабатывать наиболее эффективный путь для трафика.

На сегодняшний день большую часть рынка *Mesh*-оборудования занимают *sturtup*-компании, однако ситуация очень быстро меняется. Компании *Cisco, Motorola, Nortel, Proxim, Alvarion* (организация транспортных каналов) – вот далеко не полный перечень известных производителей, все более активно работающих в секторе *Mesh*-оборудования.

Все представленное на рынке оборудование можно условно разделить на три группы:

- группа № 1 – *Single*-радиосистемы с одиночным радиоблоком, использующие антенны круговой диаграммы направленности;
- группа № 2 – *Dual*-радиосистемы с двумя радиоблоками, использующие антенны круговой диаграммы направленности;
- группа № 3 – *Multi*-радиосистемы, использующие раздельные радиоблоки для организации транспортного и абонентского доступа с применением направленных антенн.

При использовании *Single-радио* один радиомодуль в частотном диапазоне (2,4 ГГц) применяется для организации абонентского доступа и транспортного канала между точками. Число переходов (*hops*) трафика между точками доступа должно составлять не более 3 – 4, что ограничивает возможности масштабирования сети в пределах одного кластера при организации сервисов реального времени. Несмотря на указанную специфику, сети *Mesh*, построенные на оборудовании 1-й группы, лидируют по присутствию на рынке. Оборудование характеризуется низкой стоимостью и наиболее эффективно для создания зон покрытия малого масштаба.

Самым заметным представителем этой группы является компания *Tropos Networks* (США), крупнейший производитель оборудования топологии *Mesh*5.

При использовании *Dual-радио* применяются раздельные радиомодули для организации абонентского доступа (2,4 ГГц) и транспортного канала (5,8 ГГц). Подобное решение позволяет избавиться от интерференционных помех при передаче информации между точками,

что упрощает частотное планирование сети и повышает производительность системы по транзитному трафику за счет «переноса» транспортного канала в другой частотный диапазон.

Оборудование 2-й группы выпускают почти все производители *Mesh* (*Aruba, BelAir, Cisco, Motorola, Nortel, Proxim, SkyPilot, Tropos* и др.).

Оборудование *третьей группы* (*BelAir, SkyPilot, Strix Systems* и др.) наиболее интересно по архитектурному решению. Оно построено по модульному принципу с использованием от 4 до 6 радиоблоков. Это позволяет (так же, как и в решениях *Dual*-радио) организовать разделение абонентского и транспортного потоков. Однако эффективность решения *Multi*-радио повышается за счет разделения входящего и нисходящего транспортных потоков при увеличения общего числа «транспортных» радиомодулей. Модульная архитектура (на практике это набор плат, монтируемых в типовом корпусе) допускает оперативную замену радиомодулей и позволяет производить простую модернизацию всей сети по мере развития технологической и элементной базы, включая переход на новые стандарты *WiMAX*.

16.6. Технология *WiMAX*

В основе технологии *WiMAX* (*Worldwide Interoperability for Microwave Access*) лежит протокол *IEEE* 802.16, который в отличие от других технологий радиодоступа обеспечивает высокоскоростные соединения на больших расстояниях даже при отсутствии прямой видимости объекта на отраженном сигнале.

Рис. 16.8. Организация сети *WiMAX*

Разработка стандарта 802.16 была начата институтом *IEEE* в 2000 г.

В общем виде сети *WiMAX* состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции (БС) между собой, с поставщиком сервисов и *Internet* (рис. 16.8).

Для соединения БС с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В идеальных условиях ско-

рость обмена данными может достигать 70 Мб/с, при этом не требуется обеспечения прямой видимости между БС и приёмником.

Между БС устанавливаются соединения (прямой видимости), использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигать 140 Мб/с. При этом по крайней мере одна БС подключается к сети провайдера с использованием классических проводных соединений. Однако чем большее число БС подключено к сетям провайдера, тем выше скорость передачи данных и надёжность сети в целом.

Структура сетей семейства стандартов *IEEE* 802.16 схожа с традиционными сетями *GSM* (базовые станции действуют на расстояниях до десятков километров, для их установки не обязательно строить вышки – допускается установка на крышах домов при соблюдении условия прямой видимости между станциями).

Приведённая иллюстрация даёт некоторое логическое представление об архитектуре сетей *WiMAX,* которая рассматривает набор стандартных логических функциональных модулей и стандартных интерфейсов (рис. 16.9).

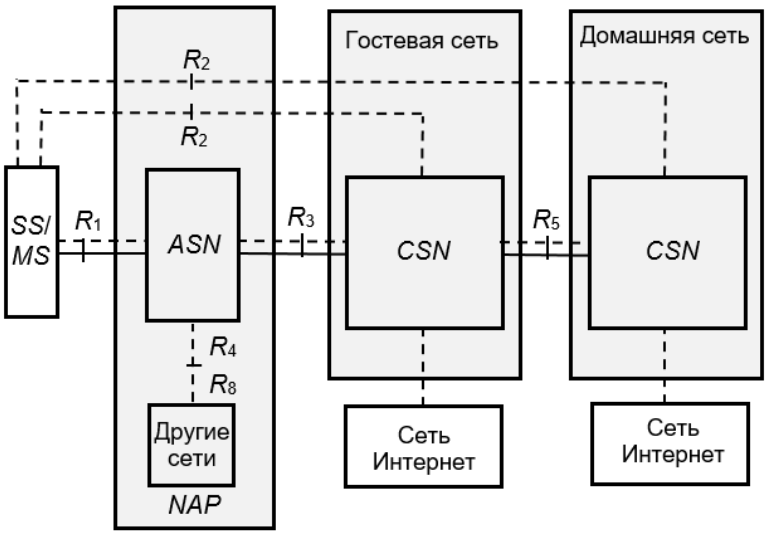


Рис. 16.9. Архитектура сетей *WiMAX*

Здесь присутствуют три основных элемента:

- множество абонентских станций *SS/MS (the Subscriber Station/Mobile Station*);

- совокупность сетей доступа (сервисная сеть доступа, *ASN* (*the Access Service Network*)) – множество базовых станций беспроводного доступа по стандарту *IEEE* 802.16 и шлюзов для связи с транспортной *IP*-сетью (т.е. с локальной или глобальной сетью передачи информации), где шлюзы – устройства соединения базовых станций всех *ASN*;

- совокупность сетей подключения *CSN* (*the Connectivity Service Network*), т.е. сеть оператора *WiMAX*, в которой реализуются функции управления авторизацией, аутентификацией и доступом, подключение абонентов *WiMAX* к глобальным *IP*-сетям, предоставление услуг, таких как *IP*-телефония, доступ к телефонным сетям общего пользования, доступ в Интернет.

Через базовые точки (*R*1 – *R*8) происходит соединение функциональных модулей. Сеть *ASN* принадлежит провайдеру сети доступа *NAP* (*Network Access Provider*) – организации, предоставляющей доступ к радиосети других (*another ASN*) сервис-провайдеров *WiMAX*. В свою очередь, сервис-провайдер *WiMAX* – организация, предоставляющая *IP*-соединения и услуги *WiMAX* конечным абонентам. В рамках данной модели уже сервис-провайдеры гостевой (*Visited NSP*) или домашней (*Home NSP*) сети *WiMAX* заключают соглашения с интернет-провайдерами, операторами других сетей доступа, соглашения о роуминге. Кроме того, обеспечивает обмен данными между сетями различных операторов.

Следует заметить, что архитектура сетей *WiMAX* не привязана к какой-либо определённой конфигурации, обладает высокой гибкостью и масштабируемостью.

Технологию *WiMAX* можно использовать для создания широкополосных соединений «последней мили», развертывания точек беспроводного доступа, организации сети между филиалами компаний и решения других задач, которые ранее были ограничены традиционными технологиями.

WiMAX технология позволяет обеспечить доступ в *Internet* со скоростями и зоной покрытия, существенно большими, чем у современных сетей *Wi-Fi*. Это сеть широкополосного беспроводного доступа, которая создается на территории целого города, а расстояние от приемника до базовой станции измеряется уже километрами.

В свою очередь, локальные сети *Wi-Fi* становятся логичным продолжением сетей *WiMAX*.

Спецификация *IEEE* 802.16 предполагает поддержку шифрования по алгоритмам *TrIPle DES*.

В Москве была запущена первая коммерческую сеть на базе беспроводной технологии *WiMAX* в диапазоне частот 2,5 – 2,7 ГГц. Сеть позволяет предоставлять услуги телефонии, доступа в *Internet* и передачи данных без использования кабельных линий.

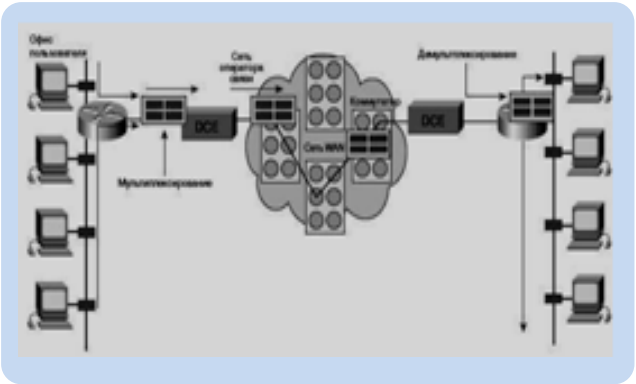
Вопросы к компьютерному тестированию

1. Какой из перечисленных стандартов *IEEE* является основой для всех последующих разработок стандартов беспроводных сетей? *IEEE* 802.9, *IEEE* 802.10, *IEEE* 802.11, *IEEE* 802.12.
2. Какие физические каналы связи использует сеть *Wireless Local Area Network*?
3. Какие из сетевых устройств образуют пикосеть?
4. Изобразить основные из возможных топологий пикосетей.
5. Что понимают под скеттерсетью, какова структурная организация такой сети?
6. Какая из версий *Bluetooth* появилась в первой половине 2003 г. и обеспечивала скорость передачи информации 2 – 3 Мб/с?
7. Из каких частей состоит интерфейс *Bluetooth*?
8. Что является терминалом *Bluetooth*-соединения?
9. Что выполняет функции управляющего устройства *Bluetooth*-соединения?
10. С использованием каких протоколов осуществляется работа *Bluetooth*?
11. В каких случаях применяется *Bluetooth*-связь?
12. Какое название получила надстройка над технологией мобильной связи *GSM*, осуществляющая пакетную передачу данных и обеспечивающая полноценный доступ в *Internet* по сетям сотовой связи?
13. Какую роль выполняет мобильный телефон, подключаемый к компьютеру при организации связи по технологии *GPRS*?

14. Каков алгоритм работы системы связи по технологии *GPRS*?
15. Протоколы каких уровней модели *OSI* используются при организации связи по технологии *GPRS*?
16. Какой вид сигнала (аналоговый, частотный, цифровой или дискретный) передается по сети при использовании технологии *Wi-Fi*?
17. Какие дополнительные устройства используются при соединении двух компьютеров по технологии *Wi-Fi*?
18. Как называется технология передачи цифровых данных по радиоканалам, изначально предназначенная для корпоративных пользователей?
19. Как называется способ объединения устройств *Wi-Fi*, когда одно устройство соединяется с другим устройством напрямую?
20. Что такое точка доступа, используемая при организации связи по технологии *Wi-Fi*?
21. В чем отличие так называемых «толстых» и «тонких» точек доступа при организации связи по технологии *Wi-Fi*?
22. От чего зависит число устанавливаемых точек доступа при организации связи по технологии *Wi-Fi*?
23. Какие недостатки присущи технологии *Wi-Fi*?
24. Какова суть технологии *MIMO* при организации сетевой беспроводной связи?
25. Какой из основных стандартов использует беспроводная технология *Mesh*?
26. Какой максимальный радиус действия технологии *WiMAX* в отсутствие прямой видимости?
27. Какой из основных стандартов лежит в основе технологии *WiMAX*?
28. В какой из технологий беспроводных сетей не требуется обеспечения прямой видимости между базовой станцией и приёмником?
29. Какие скорости обмена данными достижимы в сети *WiMAX* при соединении базовой с абонентскими станциями, при соединении между базовыми станциями?
30. Какая из известных беспроводных технологий позволяет вдвое увеличить пропускную способность канала связи?

Глава 17

АКТУАЛЬНЫЕ И СТРУКТУРИРОВАННЫЕ ЛОКАЛЬНЫЕ И ПРОМЫШЛЕННЫЕ СЕТИ



Рассматриваемые вопросы:

17.1. Актуальные локальные вычислительные сети.
17.1.1. Локальная вычислительная сеть *Novell Net Ware*.
17.1.2. Локальные сети, управляемые операционной системой *Windows NT*.
17.2. Структурированные ЛВС с использованием ассиметричных *VLAN*-технологий.
17.2.1. Виртуальная локальная сеть.
17.2.2. Варианты использования асимметричных *VLAN*.
17.3. Промышленные сети.
17.3.1. Общие понятия и определение.
17.3.2. Основные критерии выбора.
17.3.3. Протоколы.

17.1. Актуальные локальные вычислительные сети

Тип ЛВС и ее функциональные возможности во многом определяются используемыми протоколами *OSI*. Причем нижние уровни модели реализуются программно и аппаратно – интерфейсной сетевой платой, а протоколы верхних уровней поддерживаются программно – сетевой операционной системой.

Сетевая операционная система (СОС) управляет коммуникационными процессами в сети и поддерживает ее общую архитектуру. Она выделяет нужные сетевые ресурсы рабочим станциям и обеспечивает пользователю стандартный и удобный доступ к ним.

Возможно несколько вариантов организации доступа к ресурсам ЛВС:

• каждая рабочая станция имеет полный набор всех функциональных программ СОС и хранит часть из них (резидентные) в оперативной памяти, а часть (нерезидентные) в дисковой памяти;

• каждая рабочая станция имеет только набор наиболее активных программ СОС, а полный набор всех функциональных программ СОС хранится на сервере;

• рабочие станции («сетевые компьютеры») не имеют у себя никаких программ СОС, а при необходимости выполняется их удаленная загрузка с сервера.

Среди фирменных сетевых операционных систем, поддерживающих протоколы пяти верхних уровней *OSI*, наибольшее распространение получили *Net Ware* фирмы *Novell* и *Windows NT* (*Windows* 2000).

17.1.1. Локальная вычислительная сеть Novell Net Ware

Net Ware поддерживает протоколы уровней 3 – 7 *OSI* и работает с многими сетевыми платами, включая *Ethernet*, *Token Ring, Arcnet*.

Протоколы *Net Ware* для уровней 3 и 4 называются *Internetwork Packet Exchange* (*IPX* – межсетевой пакетный обмен) и *Sequenced Packet Exchange* (*SPX* – упорядоченный обмен пакетами). Оболочка *Net Ware* предоставляет сервис уровней 5, 6 и 7. В частности, основной протокол верхнего уровня *NCP* (*Net Ware Core Protocol*) обеспечивает работу основных служб СОС *Novell Net Ware* и интегрирует функции всех уровней от транспортного до прикладного. Иногда сервис, предоставляемый на 5-м и 6-м уровнях *OSI*, обеспечивается пакетом *Novell NetBIOS*. При широковещательных сообщениях, когда сервер передает информацию о сетевых службах, им предоставляемых, используется протокол *SAP* (*Service Advertising Protocol*).

Протокол *IPX* использует адрес, состоящий из номера сети, номера узла и номера сокета (внутриузлового адреса). Номер сети назначается администратором сети, номером узла является его аппаратный адрес (*MAC* – адрес сетевого адаптера или порта маршрутизатора). При коммуникациях адрес сети и адрес сокета узнаются из *SAP*, соответственно из серверных объявлений и по запросу, а адрес узла автоматически считывается из сетевого адаптера узла.

В настоящее время и у нас, и за рубежом наиболее массовые – локальные сети на базе сетевых плат *Ethernet* с операционной системой *Novell Net Ware*. Такую сеть часто называют сетью *Novell Net Ware,* реже сетью *Ethernet* (поскольку эта сетевая плата была разработана для одноименной сети).

Основной вариант локальной вычислительной сети, используемый фирмой *Novell*, базируется на тонком коаксиальном кабеле. Отрезки тонкого кабеля через специальные разъемы соединяют сетевые платы, находящиеся в компьютерах локальной вычислительной сети. В числе компьютеров сети должен быть один или несколько серверов (сеть строится по модели «файл-сервер») и рабочие станции. Максимальное количество компьютеров в сети – 87. Крупные сети делятся на сегменты – отдельные более мелкие ЛВС или отрезки кабеля с подключенными к нему компьютерами. В одном сегменте длиной до 185 м может быть до 30 компьютеров. Максимальная протяженность всей сети – около 10 км.

В последнее время большую популярность, особенно за рубежом, получил вариант сети *Novell Net Ware* на базе витой пары проводов. Он предусматривает подключение рабочих станций к файл-серверу через концентратор. Один концентратор в состоянии поддерживать работу 12 станций, расположенных на расстоянии до 120 м от него. Концентраторы можно соединять каскадами, и максимальное число сегментов в одной сети может составлять 1024. Вместо сетевых плат *Ethernet* в этих сетях используется модернизированный их вариант под кодовым обозначением *IEEE* 802.3.

Таким образом, реализация локальной вычислительной сети *Net Ware* фирмы *Novell* возможна в двух вариантах топологий:

- шинной;
- звездообразной.

Структурные схемы ЛВС на тонком кабеле и витой паре приведены на рис. 17.1 и 17.2.

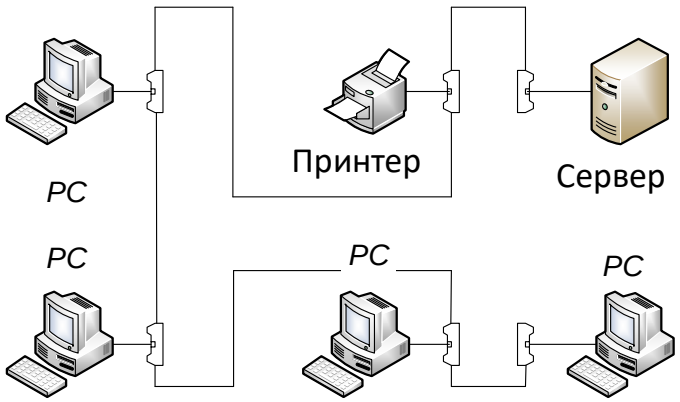


Рис. 17.1. Сеть *Net Ware* фирмы *Novell* на тонком кабеле

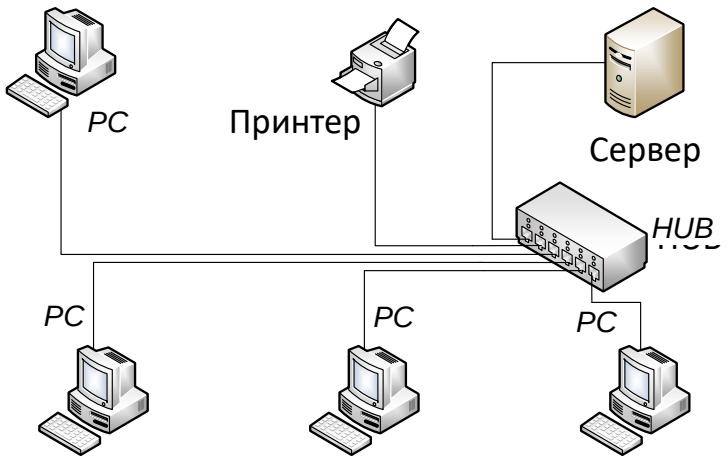


Рис. 17.2. Сеть *Net Ware* фирмы *Novell* на витой паре

Основные программные компоненты сети *Net Ware*:

• сетевая операционная система *Net Ware*, хранимая на файловом сервере;

• локальная операционная система рабочей станции.

Сетевая операционная система отвечает за управление разделяемыми ресурсами файлового сервера. Она хранится на жестком диске и загружается в оперативную память при начале работы.

Локальная операционная система компьютера размещается на рабочей станции (*Net Ware* может работать совместно с ОС *MS-DOS, OS/2, UNIX, Windows* и т.д.). Там же для обеспечения доступа к сети размещаются две программы *Net Ware – NetX.com* и *IPX.com*. Первая из них анализирует запрос прикладной программы, вторая – отправляет запрос на файл-сервер и контролирует правильность его передачи.

Для работы в сети со своей рабочей станции пользователь:

• запускает программы *NetX.com* и *IPX.com*;

• регистрируется в сети с помощью программы *Login.exe*;

• в своей операционной системе запускает нужную прикладную программу.

Основное звено ЛВС *Novell Net Ware* – файловый сервер. На нем размещаются сетевая операционная система, базы данных и прикладные программы пользователей. Поэтому файл-сервер должен быть самым мощным компьютером в сети, так как от него зависят производительность и функциональные возможности сети в целом.

Компьютер, выполняющий функции рабочей станции, должен обеспечить пользователю возможность решения всех его прикладных задач. Требования к рабочим станциям более скромные, чем к файл-серверу.

Если рабочая станция ориентирована только на сетевой режим работы, то ей, в сущности, не нужен ни винчестер, ни гибкие диски. Появляется возможность использовать *бездисковые рабочие станции*. Операционная система на такой станции загружается дистанционно под управлением файл-сервера из постоянного запоминающего устройства, установленного в сетевой плате рабочей станции.

17.1.2. Локальные сети, управляемые операционной системой Windows NT

Операционная система *Windows NT* имеет две сетевые модификации:

1. *Windows NT Workstation*;
2. *Windows NT Server*.

Windows NT Workstation для установки на рабочих станциях с возможностью организации одноранговых сетей. Есть возможность создать и сеть типа «клиент-сервер», но с весьма ограниченными возможностями.

Все компьютеры в одноранговой сети равноправны и могут выступать как в роли пользователей (клиентов) ресурсов, так и в роли их поставщиков (серверов).

На рис. 17.3 конфигурация из трех персональных компьютеров, соединенных при помощи сетевых адаптеров и кабеля. На компьютерах *PC*1 и *PC*2 установлена локальная операционная система *Windows*, а на компьютере *PC*3 – *Windows NT Workstation*.

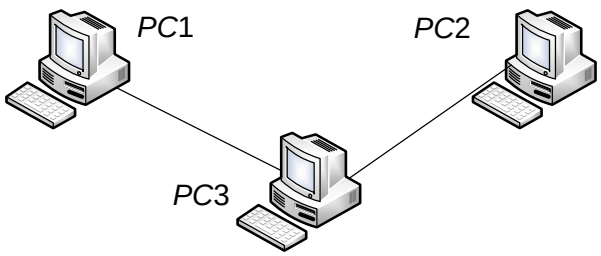


Рис. 17.3. Одноранговая сеть из трех ПК

В одноранговой сети каждый компьютер может выполнять свою конкретную функцию, и его конфигурация определяется решаемыми на нем задачами. Некоторые ресурсы одного компьютера могут быть предоставлены в общее пользование, например принтер, подключенный к *PC*2.

Совершенно другую роль может играть *PC*3 с ОС *Windows NT Workstation*. Этот компьютер – самый мощный в рассматриваемой конфигурации сети, поэтому он может использоваться для хранения информации, которая необходима пользователям постоянно, то есть выступать в качестве невыделенного сервера файлов и выполнять функции высокопроизводительной рабочей станции.

Windows NT Server (например, *Windows Server* 2000) позволяет реализовать полноценную двухранговую сеть. Сервер сети при этом может выступать как сервер приложений, файл-сервер, сервер печати, сервер связи, сервер *Internet*, сервер удаленного доступа и т. д.

Сети на базе *Windows NT Server* используют доменную модель, в основе которой лежит понятие домена – совокупности компьютеров, характеризующейся наличием общей базы учетных записей пользователей и единой политикой осуществления защиты.

Доменный метод организации упрощает централизованное управление сетью и позволяет использовать *Windows Server* 2000 в качестве сетевой операционной системы предприятия любого масштаба. Доменная служба каталогов основана на однократной регистрации пользователя в сети для доступа ко всем серверам и ресурсам информационной системы независимо от места регистрации.

Для организации доменной структуры в сети и установления в ней определенных отношений и правил используется сервер – *главный контроллер домена,* на котором хранится база учетных записей пользователей этого домена с уникальными параметрами и их привилегиями. Когда пользователь рабочей станции регистрируется в сети, происходит его идентификация на главном контроллере или на одном из резервных контроллеров домена. Если пароль и имя пользователя совпадают с введенным, то пользователь регистрируется в домене.

Сети малых размеров могут состоять из одного домена. Однако для средних и больших предприятий сеть, как правило, состоит из нескольких доменов, повторяя, например организационную структуру

предприятия. Механизм взаимодействия доменов основан на установлении доверительных отношений – так называется связь между доменами, позволяющая пользователям одного домена обращаться к ресурсам другого домена.

По умолчанию пользователи одного домена не имеют прав доступа к ресурсам другого домена. Однако имеется механизм предоставления пользователям различных доменов возможности совместно использовать ресурсы путем установления доверительных отношений между доменами (рис. 17.4).

Доверительные отношения могут быть как двусторонними, так и односторонними. При двусторонних отношениях пользователь любого из двух доменов имеет доступ к ресурсам серверов, находящихся в соседнем домене. При односторонних доверительных отношениях пользователь, находящийся в доверяемом домене, имеет доступ к серверам домена-доверителя, но не наоборот.

Существуют две основные модели установления доверительных отношений:

- модель с мастер-доменами;
- модель полностью доверительных отношений.

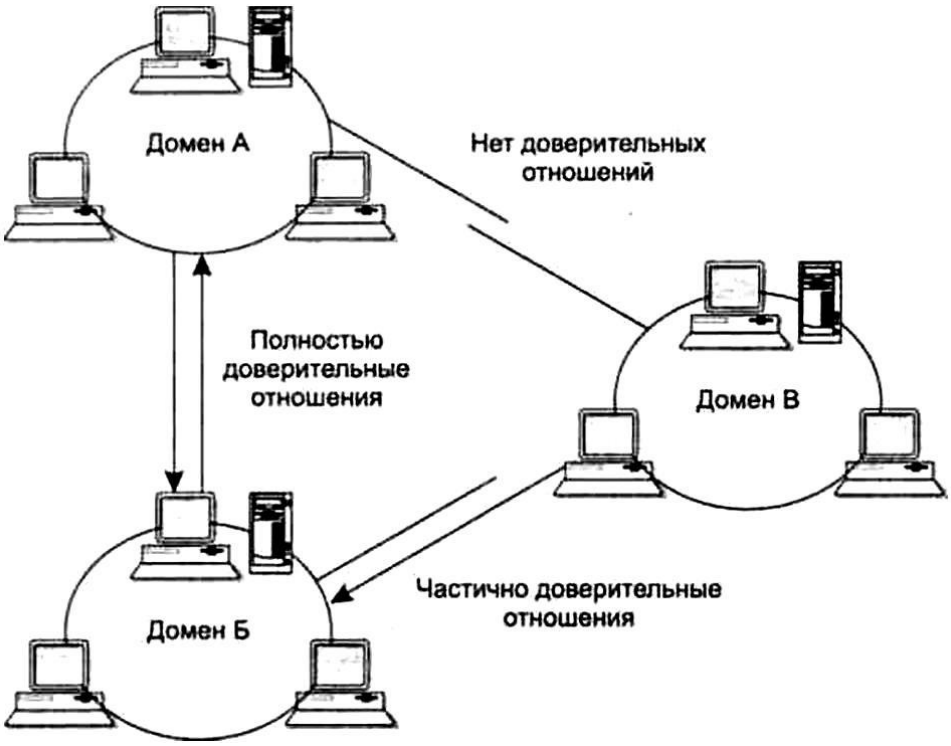


Рис. 17.4. Доверительные связи доменов в сети

В модели с мастер-доменами один или несколько доменов объявляются главными и в каждом из них хранятся учетные записи подмножества пользователей сети. Остальные домены являются вторичными, так называемыми ресурсными доменами. Все они доверяют каждому из главных доменов или только некоторым из них.

В модели с полностью доверительными отношениями все домены равноправны и из каждого из них может осуществляться управление сетью. Каждый из доменов содержит как учетные записи, так и разделяемые ресурсы. Данная модель чрезвычайно сложна в управлении, поскольку в ней необходимо устанавливать большое число доверительных отношений.

Каждому пользователю в сети соответствует персональная учетная запись, параметры которой определяют его права и обязанности в домене. Учетная запись содержит такую информацию о пользователе, как его имя, пароль и ограничения на его деятельность в сети.

Учетные записи бывают двух типов: глобальные и локальные. Локальные учетные записи определяют права пользователей на конкретном компьютере и не распространяются на домен. При использовании локальной учетной записи пользователь получает доступ только к ресурсам своего компьютера. Для доступа к ресурсам домена пользователь должен зарегистрироваться в домене, воспользовавшись своей глобальной учетной записью.

Возможна и так называемая сквозная регистрация, то есть пользователь, регистрируясь один раз в своем домене, получает доступ к ресурсам доверяющего домена, в котором у него нет персональной учетной записи.

Создавать, модифицировать учетные записи и управлять ими администратор сети может с помощью программы *User Manager for Domains*. При создании новой учетной записи администратор определяет следующие параметры: пароль и правила его модификации, локальные и глобальные группы; в них входят пользователь и рабочие станции, с которых он может регистрироваться, разрешенные часы работы, срок действия учетной записи и др.

Наряду с базовой ОС *Windows Server* существуют и ее модификации: ОС *Windows Advanced Server* и ОС *Windows Datacenter Server*, имеющие увеличенную масштабируемость и производительность.

17.2. Структурированные ЛВС с использованием асимметричных *VLAN*-технологий

Структурированные ЛВС предназначены для обеспечения более высокой степени защищенности информации от несанкционированного доступа по сравнению с традиционными (распределенными) сетями, а также для повышения производительности сети и организации более эффективного управления компонентами сети и информационными потоками.

Создание такой ЛВС стало возможным благодаря использованию во всех коммутационных узлах интеллектуальных коммутаторов, работающих на канальном (2-м) уровне модели *OSI*. Кроме того, они должны поддерживать передачу маркированных (*tegging*) пакетов (стандарт *IEEE* 802.1*q*), а также асимметричные виртуальные локальные сети *VLAN* (например, коммутаторы *DES*-3226*S* и *DES*-3526 компании *D-Link*). Термин *VLAN* это сокращение от *Virtual Local-Area Network* и наиболее часто связан с коммутаторами.

17.2.1. Виртуальная локальная сеть

Виртуальная локальная сеть (VLAN) – это сегмент общей сети, который представляет собой объединение портов различных коммутаторов в логическую группу, образующую безопасный автономный широковещательный домен. Основная цель разбиения сети на несколько *VLAN* – ограничение распространения широковещательных пакетов, поскольку их передача между различными *VLAN* невозможна. Распределенный по зданию персонал подразделения может быть объединен в отдельный *VLAN* для совместного использования ресурсов, как будто он подключен к одному общему сетевому сегменту.

Логическая группировка сетевых ресурсов в виртуальные локальные сети освобождает сетевых администраторов от ограничений существующей сетевой топологии и кабельной инфраструктуры и упрощает администрирование. Виртуальные сети создают виртуальные границы, которые могут пересекаться только при прохождении через маршрутизатор. Таким образом, стандартные технологии защиты, применяемые в маршрутизаторах, могут использоваться для ограничения доступа к различным виртуальным сетям.

В качестве практического примера рассмотрим схему структурированной ЛВС некоторого типичного предприятия, представленную на рис. 17.5. В ее основу положена древовидная топология.

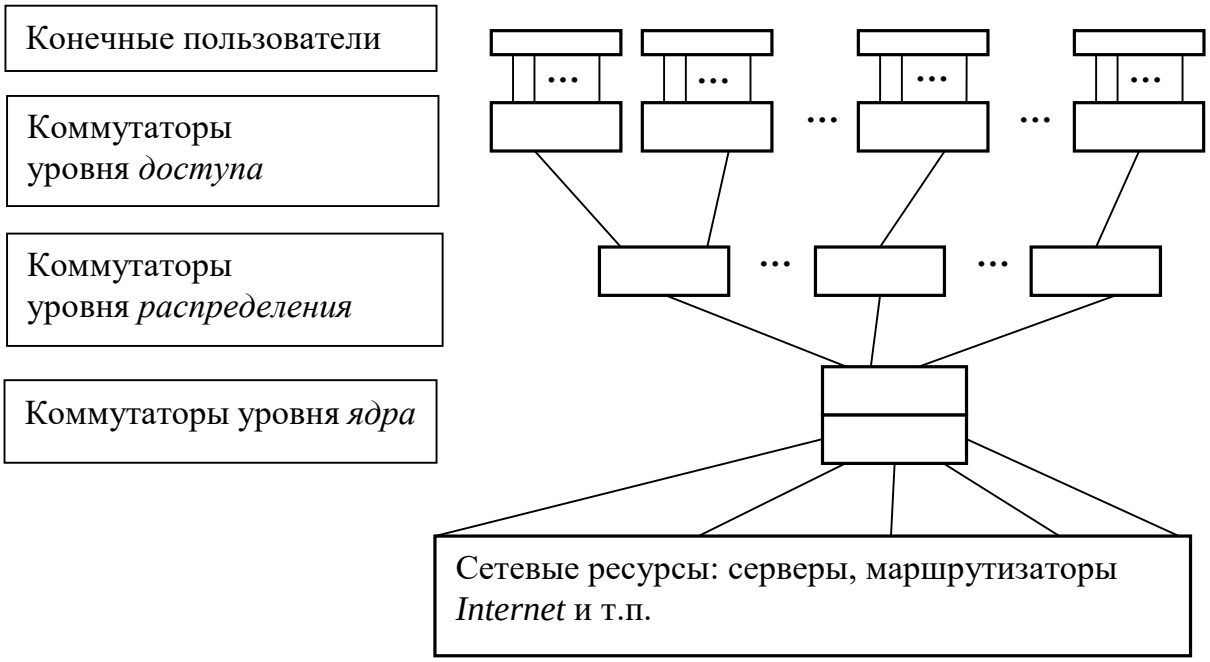


Рис. 17.5. Функциональная схема структурированной ЛВС

Коммутаторы уровня ядра устанавливаются в аппаратной (серверной), где также, как правило, располагаются все сетевые ресурсы: серверы (файл-серверы, серверы приложений, почтовые серверы и т.п.), маршрутизатор доступа в *Internet* и т.п. Эти коммутаторы формируют единую производительную информационную магистраль предприятия.

Коммутаторы уровня распределения обычно располагаются в коммутационных помещениях и/или шкафах, установленных на разных этажах или в разных секциях здания.

Коммутаторы уровня доступа, как правило, располагаются там же, и к ним подходят линии от персональных компьютеров пользователей, сетевых принтеров и иных оконечных устройств. Коммутаторы уровня доступа обычно служат для увеличения количества портов, требуемых для подключения ПК пользователей.

Коммутаторы «ядра» удобно объединить в *стек*. Стек коммутаторов ядра соединяется с коммутаторами уровня распределения, при-

чем обычно в этом случае используется агрегирование каналов или, иначе, объединение портов в *транк*, состоящий из нескольких (2 – 8) кабельных линий. Это позволяет, с одной стороны, расширить полосу пропускания соединения, а с другой – обеспечивает повышенную надежность соединения за счет дублирования каналов.

Задача подобной организации состоит в том, чтобы иметь возможность обеспечить доступ к различным комбинациям сетевых ресурсов пользователям в зависимости от их прав доступа, организационной принадлежности и политик безопасности без прокладки дополнительных кабельных линий. При этом должна быть исключена возможность трафика между компьютерами различных подразделений предприятия.

Эта задача решается с помощью *асимметричных VLAN*, построенных на основе меток в дополнительном поле пакета (стандарт *IEEE* 802.1q).

17.2.2. Варианты использования асимметричных VLAN

Рассмотрим решение данной задачи на примере простейшей сети, изображенной на рис. 17.6.

Имеются три сервера *S*1, *S*2 и *S*3. Эти сетевые ресурсы подключены к коммутатору «ядра» *SW*1 (*DES*-3226*S* или *DES*-3526), который, в свою очередь, соединен с коммутатором уровня распределения *SW*2 (*DES*-3226*S* или *DES*-3326*S*). Для каждого сервера на базе портов 1, 2 и 3 коммутатора *SW*1 создается отдельный *VLAN* – соответственно *VS*1 (включает порт 1), *VS*2 (включает порт 2) и *VS*3 (включает порт 3). Создаем еще два *VLAN* – *VS*12 (включает порт 4) и *VS*23 (включает порт 5), и с помощью настроек асимметричных *VLAN* формируем пути для трафика, показанные на рисунке стрелками (сплошные линии). В этом случае ПК $PC12_1$, который подключен к порту 4 коммутатора *SW*1, входящему в *VLAN VS*12, будут доступны данные на серверах *S*1 и *S*2, а ПК $PC23_1$, который подключен к порту 5 коммутатора *SW*1, входящему в *VLAN VS*23, будут доступны данные на серверах *S*2 и *S*3. В то же время трафик между *VS*12 и *VS*23 будет запрещен (перечеркнутая стрелка); следовательно, информация с *S*3 и $PC23_1$ будет недоступна для $PC12_1$, и информация с *S*1 и $PC12_1$ будет недоступна для $PC23_1$, а ресурсы сервера *S*2 будут доступны как $PC12_1$, так и $PC23_1$.

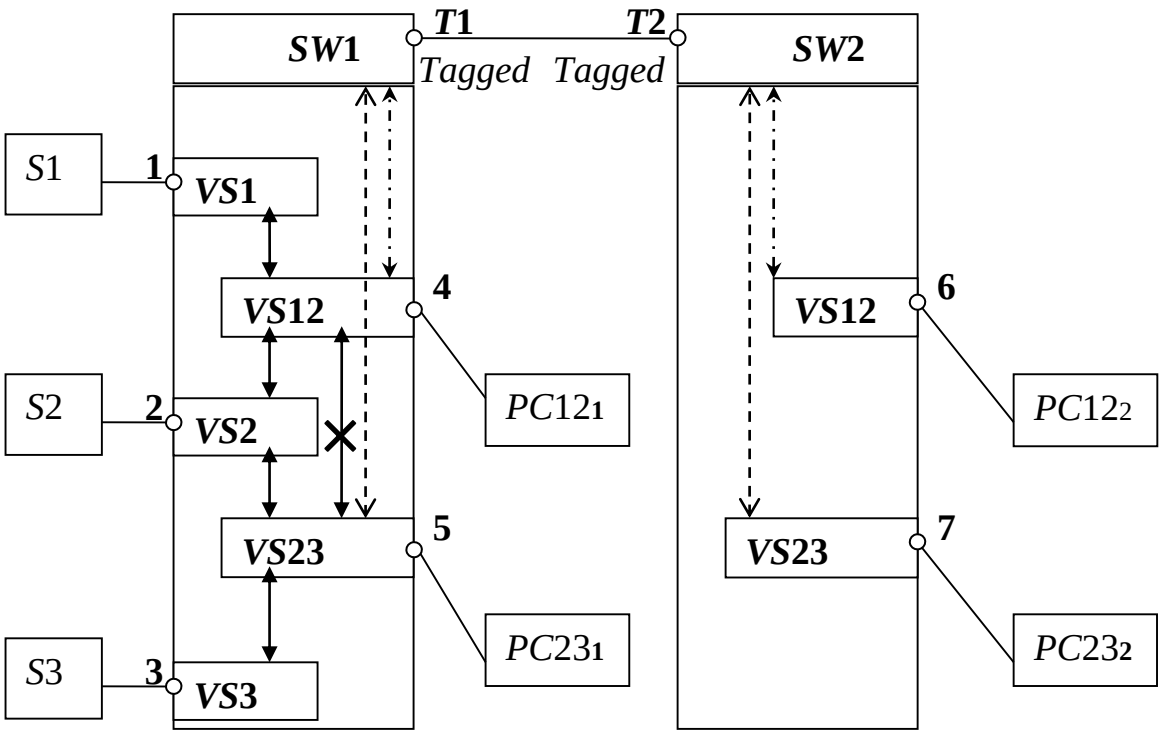


Рис. 17.6. Использование асимметричных *VLAN* для создания разделенных ресурсов

Поскольку коммутатор *SW*1 является коммутатором «ядра», то компьютеры пользователей *PC*12 и *PC*23 желательно подключать к другому коммутатору – коммутатору уровня распределения, например *SW*2, или коммутатору уровня доступа (на рисунке не показан). В этом случае необходимо распространить действие *VS*12 и *VS*23 на коммутатор *SW*2. Для этого воспользуемся таким свойством коммутаторов, как поддержка *VLAN* на основе меток в дополнительном поле пакета – стандарт *IEEE* 802.1*q*.

Казалось бы, можно решить эту задачу следующим образом. На коммутаторе *SW*2 создаем два аналогичных *VLAN* – *VS*12 и *VS*23 и соединяем эти коммутаторы, например портами *T*1 и *T*2. Отмечаем эти порты как *Tagged* (маркирующие) и включаем их в состав *VS*12 и *VS*23 на обоих коммутаторах. Предполагаемый трафик обозначен на рисунке стрелками из пунктирных линий. Однако такое решение оказывается неверным, поскольку поддержка асимметричных *VLAN* ограничена автономными коммутаторами, а мы пытаемся распространить действие асимметричных *VLAN* на два коммутатора. Верное решение приведено на рис. 17.7.

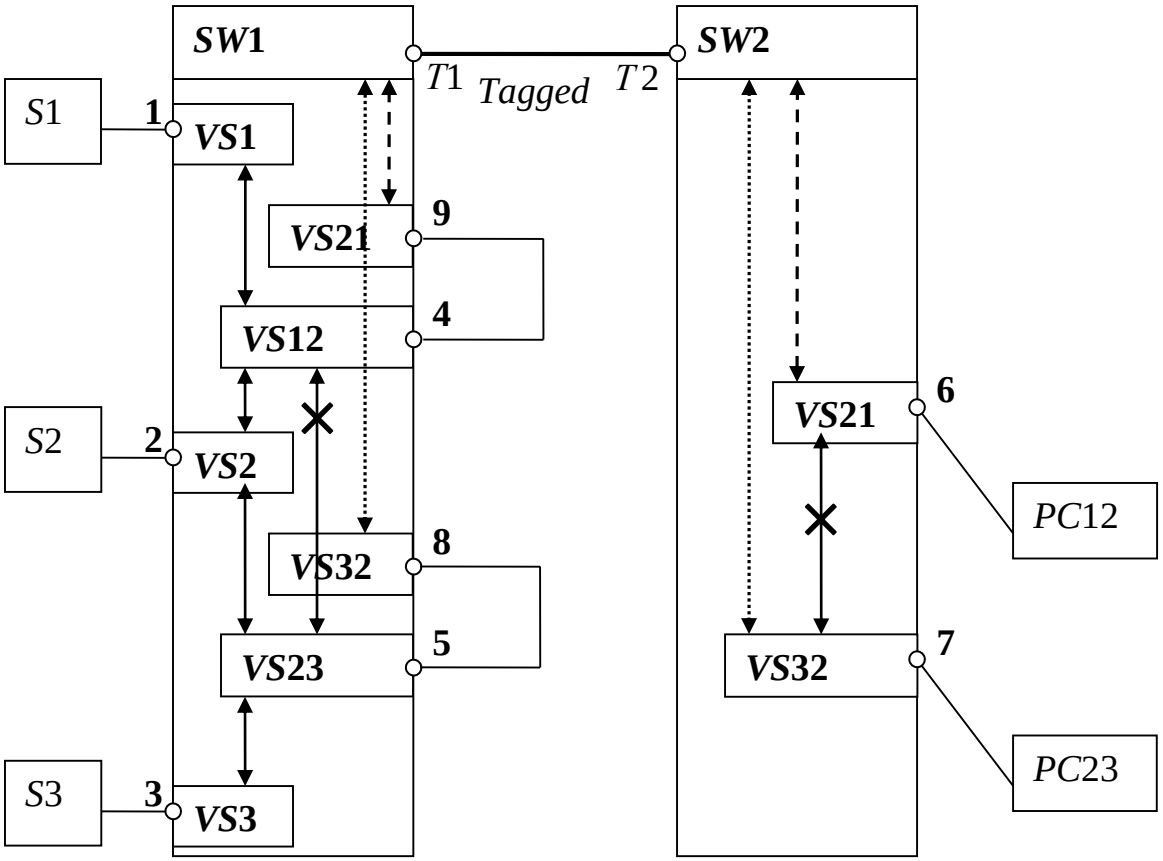


Рис. 17.7. Организация передачи сетевых ресурсов
на уровень распределения – вариант I

На коммутаторах *SW*1 и *SW*2 создаем по два дополнительных *VLAN* – *VS*21 на портах 6 и 9 и *VS*32 на портах 7 и 8 соответствующих коммутаторов. Соединяем эти коммутаторы посредством маркирующих (*Tagged*) портов *T*1 и *T*2. Порты 5 и 8, а также 4 и 9 коммутатора *SW*1 соединяем перемычками. В результате организуется связь между портами различных коммутаторов, принадлежащих одноименным *VLAN*. Такую организацию виртуальных сетей будем в дальнейшем называть *распределенной (мостовой) VLAN*. В этом случае трафик будет осуществляться так, как показано на рисунке стрелками. Тогда ПК *PC*12 будет иметь доступ к ресурсам серверов *S*1 и *S*2, а ПК *PC*23 будет иметь доступ к ресурсам серверов *S*2 и *S*3, в то же время трафик между *PC*12 и *PC*23 оказывается невозможен (перечеркнутая стрелка).

Для увеличения полосы пропускания соединения коммутаторов *SW*1 и *SW*2 следует применить агрегирование портов. Коммутатор уровня распределения, например *SW*2, желательно использовать для создания «распределенных» *VLAN*, имеющих на этом коммутаторе

всего один порт, а для увеличения числа портов, предназначенных для включения в эти *VLAN* конечных пользователей, следует использовать коммутаторы уровня доступа, подключаемые, например к портам 6 и 7 коммутатора *SW*2. Для увеличения полосы пропускания соединения коммутаторов уровня распределения и коммутаторов уровня доступа можно также использовать агрегирование портов.

В ряде случаев возникает необходимость передавать каждый сетевой ресурс на уровень распределения и уже там организовывать доступ к этому ресурсу, исключая трафик между его потребителями. Например, необходимо предоставить доступ к *Internet* ПК подразделений П1 и П2 предприятия, исключив возможность трафика между компьютерами этих подразделений. На рис. 17.8 приведен простейший вариант такой сети.

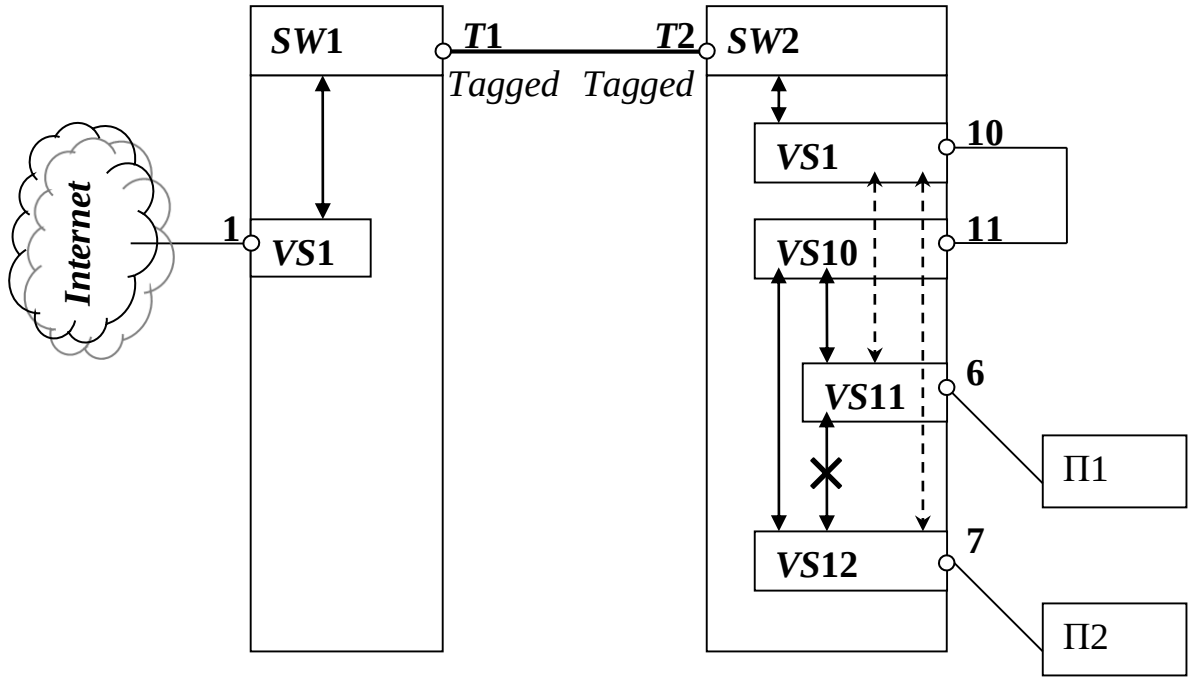


Рис. 17.8. Организация передачи сетевого ресурса на уровень распределения – вариант II

Создаем «распределенную» *VLAN VS*1 на обоих коммутаторах описанным выше способом. На коммутаторе *SW*2 создаем два пользовательских *VLAN* подразделений – *VS*11 и *VS*12 на портах соответственно 6 и 7. Как было отмечено выше, поддержка асимметричных *VLAN* ограничена автономными коммутаторами. Поэтому, если непосредственно включить порты 6 и 7 в состав *VS*1 в качестве асимметричных *VLAN*,

то трафик, обозначенный стрелками из пунктирных линий, не будет выполняться, поскольку в этом случае асимметричный *VS*1 будет располагаться на нескольких коммутаторах. Для реализации поставленной задачи на коммутаторе *SW*2 создаем дополнительный *VLAN VS*10, в состав которого включаем порты 6 и 7, одновременно принадлежащие виртуальным сетям *VS*11 и *VS*12, а в состав *VS*11 и *VS*12 включаем порт 11, принадлежащий *VS*10; иными словами, создаем асимметричный *VLAN*. Порты 10 и 11 коммутатора *SW*2 соединяем перемычкой. В результате будет соблюдаться требование, ограничивающее действие асимметричного *VLAN* одним коммутатором, и в то же время будет организован совместный доступ компьютеров подразделений П1 и П2 к *Internet* при запрете трафика между ПК подразделений (перечеркнутая стрелка).

Рекомендации. Оба рассмотренных способа организации передачи сетевых ресурсов с уровня ядра на уровень распределения имеют свои достоинства и недостатки.

Первый способ позволяет создавать необходимые комбинации сетевых ресурсов в одном месте и передавать их только на те коммутаторы уровня распределения, где они требуются. В этом случае существенно сокращается трафик между коммутаторами ядра и коммутаторами уровня распределения. Кроме того, данный способ не требует установки на уровне распределения коммутаторов, поддерживающих асимметричные *VLAN*; достаточно коммутатора, поддерживающего обычный стандарт *IEEE* 802.1*q*. К недостаткам такого способа следует отнести необходимость установки на уровне ядра коммутаторов с большим количеством портов или создания стека коммутаторов ядра. Также изменение конфигурации коммутаторов ядра в процессе эксплуатации, что обычно требуется при изменении топологии сети, может повлиять на работу всех пользователей.

Второй способ удобен тем, что на всех коммутаторах уровня распределения можно иметь сразу все сетевые ресурсы, изначально подключенные к коммутаторам ядра, и по мере необходимости создавать из них требуемые комбинации лишь для групп пользователей, подключенных к конкретному коммутатору уровня распределения. В этом случае переконфигурирование коммутатора может затронуть лишь подключенных к нему пользователей. К недостаткам такого способа следует отнести повышенный трафик между коммутаторами ядра и

коммутаторами уровня распределения, поскольку доступ к сетевым ресурсам распространяется сразу на все коммутаторы уровня распределения. Кроме того, все коммутаторы уровня распределения должны поддерживать асимметричные *VLAN*. Но основной недостаток второго способа заключается в том, что он не позволяет простым образом обеспечивать связь между ПК, подключенными к различным коммутаторам уровня распределения, например, в случае, когда ПК одного подразделения предприятия располагаются на разных этажах и физически подключены к различным коммутаторам уровня распределения.

Опыт построения большой распределенной ЛВС показывает, что при проектировании такой сети следует предусмотреть возможность использования сразу обоих способов организации передачи сетевых ресурсов на уровень распределения, т.е. на уровне ядра следует создавать стек из коммутаторов, поддерживающих асимметричные *VLAN*, и на уровне распределения использовать также коммутаторы, поддерживающие асимметричные *VLAN*. Кроме того, для обеспечения повышенной защищенности системы управления настройками коммутаторов ЛВС от несанкционированного доступа следует создать на всех коммутаторах сети отдельную распределенную *VLAN* и настроить коммутаторы так, чтобы управлять настройками всех коммутаторов сети было возможно лишь со станции управления сетью, подключенной только в эту *VLAN*.

Предложенный вариант построения локальной вычислительной сети обладает следующими свойствами: структурность, универсальность и избыточность.

Основные достоинства рассмотренного варианта построения ЛВС:

- обеспечение высокой степени защищенности информации от несанкционированного доступа за счет создания для каждого подразделения предприятия или отдельного пользователя виртуальных локальных сетей, ограничивающих трафик в пределах отдельной *VLAN*;
- возможность размещения всех основных вычислительных ресурсов (серверов) в одной аппаратной (серверной) позволяет обеспечить требуемый уровень их защищенности от внешних воздействий и удобство обслуживания;
- возможность предоставления доступа к любым из имеющихся сетевых ресурсов на каждом коммутаторе уровня распределения без проведения работ по прокладке дополнительных кабельных линий;

• структурная гибкость сети, позволяющая быстро менять строение сети, наращивая или подстраивая ее под изменяющуюся структуру предприятия без проведения работ по прокладке дополнительных кабельных линий;

• масштабируемость сети, что дает возможность легко наращивать вычислительные ресурсы сети простым подключением дополнительных серверов и других сетевых элементов к стеку коммутаторов ядра;

• возможность подключения локальных средств архивизации в любой удобной точке сети, что позволяет расположить устройства архивизации как с учетом минимизации нагрузки на сеть, так и в месте, наиболее защищенном от пожара, затопления и т.п.;

• невысокая стоимость решения и оптимальное соотношение показателя цена/качество позволяют при малом бюджете развертывать гибкую, высокозащищенную информационную инфраструктуру.

17.3. Промышленные сети

В 1980-е гг. прошлого века произошел постепенный переход от аналоговой технологии приборной связи к цифровой. До этого времени в связи с высокой ценой ЭВМ и относительно низким уровнем автоматизации производства системы обмена данными строились по традиционной централизованной схеме, в которой имелось одно мощное вычислительное устройство и огромное количество кабелей, посредством которых осуществлялось подключение датчиков и исполнительных механизмов. В условиях бурно растущего производства микропроцессорных устройств альтернативным решением стали цифровые промышленные сети (*Fieldbus*), состоящие из многих узлов, обмен между которыми производится цифровым способом.

17.3.1. Общие понятия и определение

Промышленная сеть – сеть передачи данных, связывающая различные датчики, исполнительные механизмы, промышленные контроллеры и используемая в промышленной автоматизации. Термин употребляется преимущественно в АСУ ТП. Устройства используют сеть:

- для передачи данных, настройки, ввода в эксплуатацию и диагностики оборудования АСУ ТП;

- питания датчиков и исполнительных механизмов;
- передачи данных между датчиками и исполнительными механизмами, минуя центральный контроллер;
- связи между датчиками, исполнительными механизмами, ПЛК и АСУ ТП верхнего уровня;
- связи между контроллерами и системами человеко-машинного интерфейса (операторскими системами).

В промышленных сетях для передачи данных применяют кабели, оптоволоконные линии, беспроводную связь. Промышленные сети могут взаимодействовать с обычными компьютерными сетями, в частности использовать глобальную сеть *Internet*.

Термин *полевая шина* – дословный перевод английского термина «*Fieldbus*». Термин *промышленная сеть* – более адекватный перевод, и в настоящее время именно он используется в профессиональной технической литературе.

На сегодняшний день на рынке представлено около сотни различных типов промышленных сетей, протоколов и интерфейсов, применяемых в системах автоматизации, среди которых наиболее известны *Modbus, Profibus, Interbus, Bitbus, CAN, LON, HART, Foundation Fieldbus, DH+, Control Net, Device Net, Ethernet* и др.

Использование промышленной сети позволяет расположить узлы, в качестве которых выступают контроллеры и интеллектуальные устройства ввода-вывода, максимально приближенно к оконечным устройствам (датчикам и исполнительным механизмам), благодаря чему длина аналоговых линий сокращается до минимума, каждый узел промышленной сети выполняет несколько функций:

- прием команд и данных от других узлов промышленной сети;
- считывание данных с подключенных датчиков;
- преобразование полученных данных в цифровую форму;
- отработку запрограммированного технологического алгоритма;
- выдачу управляющих воздействий на подключенные исполнительные механизмы по команде другого узла или согласно технологическому алгоритму;
- передачу накопленной информации на другие узлы сети.

АСУ ТП на базе промышленных сетей по сравнению с традиционными централизованными системами имеют несколько особенностей.

1. *Существенная экономия кабельной продукции*: вместо километров дорогих кабелей требуется несколько сот метров дешевой витой пары. Сокращаются также расходы на вспомогательное оборудование (кабельные каналы, клеммы, шкафы).

2. *Повышение надежности системы управления*: цифровой метод передачи данных намного превосходит аналоговый. Передача в цифровом виде малочувствительна к помехам и гарантирует доставку информации благодаря специальным механизмам, встроенным в протоколы промышленных сетей (контрольные суммы, повтор передачи искаженных пакетов данных).

Повышение надежности также связано с распределением функций контроля и управления по различным узлам сети. Выход из строя одного узла не влияет либо влияет незначительно на отработку технологических алгоритмов в остальных узлах. Для критически важных технологических участков возможно дублирование линий связи или наличие альтернативных путей передачи информации. Это позволяет сохранить работоспособность системы в случае повреждения кабельной сети.

3. *Гибкость и модифицируемость*. Добавление или удаление отдельных точек ввода-вывода и даже целых узлов требует минимального количества монтажных работ и может производиться без остановки системы автоматизации. Переконфигурация системы выполняется на уровне программного обеспечения и также занимает минимальное время.

4. *Использование принципов открытых систем и технологий*, что позволяет успешно интегрировать в единую систему изделия от различных фирм-производителей.

Цифровая сеть *Fieldbus* пришла на смену ранее централизованной аналоговой технологии. Каждое *Field*-устройство способно самостоятельно выполнять ряд функций по самодиагностике, контролю и обслуживанию функций двунаправленной связи. Доступ к устройствам возможен не только со стороны инженерной станции, но и со стороны аналогичных ему устройств (например, других контроллеров). При построении сетей чаще всего используется шинная структура, в которой все устройства подсоединены к общей среде передачи данных, или шине. Таким образом, адресат получает свой информационный пакет без посредников. Подключение дополнительных узлов к

шине достаточно просто. Физически шина выполняется на основе кабеля витая пара или оптоволокна.

Управление технологическим процессом в реальном времени требует такой организации обработки измерительной информации, которая обеспечивает своевременное принятие необходимых управляющих воздействий. В промышленных сетях, как и в АСУТП, применяются три основные архитектуры сетевого обмена: «Клиент/Сервер», «*Master/Slave*» и обмен с помощью широковещательных пакетов.

Архитектура «Клиент/Сервер» используется в большинстве случаев. Взаимодействие происходит по принципу «запрос – ответ». Каждый запрос попадает в буфер, прежде чем поступить в процессор на обработку. Время ответа на запросы возрастает с ростом числа клиентов по экспоненциальному закону. Это архитектура с гарантированной, хотя и медленной доставкой сообщений. О режиме реального времени говорить нельзя, так как неизвестно время нахождения запроса в очереди.

Архитектура «*Master/Slave*» (господин/слуга) применяется обычно на нижнем уровне автоматизации (протоколы *Bitbus, Profibus* и др.). Центральный ПК, или ПЛК (*Master*), периодически опрашивает все необходимые станции (*Slave*). Получив запрос, *Slav*e выполняет какие-либо действия в зависимости от полученных данных (например, замыкает реле) и посылает ответ. *Master* получает ответ, обрабатывает его и переходит к следующему узлу. В этой архитектуре реализуется режим реального времени.

Архитектура обмена с помощью широковещательных пакетов применяется для периодического обмена данными с большой интенсивностью, например от управляющей станции к остальным станциям промышленной сети. Но при этой архитектуре возможны ошибки.

Большое разнообразие открытых промышленных сетей, интерфейсов и протоколов связано с многообразием требований, автоматизируемых технологических процессов. Эти требования не могут быть удовлетворены универсальным и экономически оптимальным решением. Очевидно, что ни одна из существующих сетей не станет единственной. При выборе типа промышленной сети необходимо уточнять, для какого именно уровня автоматизации этот выбор осуществляется.

17.3.2. Основные критерии выбора

Как отмечалось выше, понятие «*field*» определяет область, связанную непосредственно с производственной зоной, где работают контроллеры, датчики (давления, температуры, уровня и т.д.) и исполнительные механизмы (клапаны, реле и т.д.). Задача полевой шины, или промышленной сети (*fieldbus*), состоит в организации физической и логической связи датчиков с системным интеллектом, роль которого выполняют промышленные компьютеры таким образом, чтобы информация с этого уровня была доступна общезаводской информационной системе.

Промышленные сети должны полностью удовлетворять запросам потребителей по модульности, надежности, защите от внешних помех, простоте в построении, монтаже и программировании логики работы.

Сегодня говорить о некоей универсальной промышленной сети не приходится. Однако требования к ней уже сегодня становятся определенными и понятны классы прикладных задач, которые надо решать с ее помощью.

Автоматизация на общезаводском уровне. Здесь необходимы следующие качества: высокая скорость передачи, короткое время реакции на события, длина линий до 300 метров. На этом уровне для большинства приложений понятие «взрывозащищенность» не является обязательным.

Автоматизация на уровне управления конкретными технологическими процессами. Здесь необходимы следующие качества: среднее время цикла опроса датчиков (до 100 мс), длина линий связи до 1500 м с реализацией механизмов внутренней защиты (*intrinsically safe*).

Предпочтительность того или иного сетевого решения как средства транспортировки данных можно оценить по следующей группе критериев:

- объем передаваемых полезных данных;
- время передачи фиксированного объема данных;
- удовлетворение требованиям задач реального времени;
- максимальная длина шины;
- допустимое число узлов на шине;
- помехозащищенность;
- денежные затраты в расчете на узел.

Часто улучшение по одному параметру может привести к снижению качества по-другому, то есть при выборе того или иного протокольного решения необходимо следовать принципу разумной достаточности. В зависимости от области применения весь спектр промышленных сетей можно разделить на два уровня:

- *Fieldlevel* (промышленные сети этого уровня решают задачи по управлению процессом производства, сбора и обработки данных на уровне промышленных контроллеров);
- *Sensor/actuator level* (задачи сетей этого уровня сводятся к опросу датчиков и управлению работой разнообразных исполнительных механизмов).

Другими словами, необходимо различать промышленные сети для системного уровня (*Fieldbus*) и датчикового уровня (*Sensorbus/actuatorbus*). Сравнение этих двух классов в самом общем виде можно получить по критериям из табл. 17.1.

Табл. 17.1. Сравнение классов промышленных сетей

Основные критерии	***Fieldbus***	***Sensorbus***
1. Расширение сети	От 100 м до 1 км	До 100 м
2. Время цикла	От 10 мс до 10 с	От 1 мс до 1 с
3. Объем передаваемых данных за цикл	От 8 байт до нескольких сотен байт	От 1 до 8 байт
4. Доступ к шине	Фиксированный/свободный	Свободный
5. Цена среды передачи	Низкая	Очень низкая

17.3.3. Протоколы

На сегодняшний день спектр протоколов для обоих этих классов довольно широк. Но надо помнить, что область их применения лежит на одном из двух уровней.

Типичные представители открытых промышленных сетей: *Profibus (Process Fieldbus), Bitbus.*

Типичные открытые сенсорные (датчиковые) сети:

ASI (Actuator/Sensor Interface), Interbus-S, Profibus-DP (Profibus for Distributed PerIPhery), Sercos interface.

Типичные открытые сети для обоих уровней применения:

CAN (Controller Area Network), FIP (Factory Instrumentation Protocol), LON (Local Operating Network).

На рис. 17.9 представлена обобщенная сетевая структура, показывающая в общем виде возможное использование того или иного протокола на определенных уровнях условного промышленного предприятия.

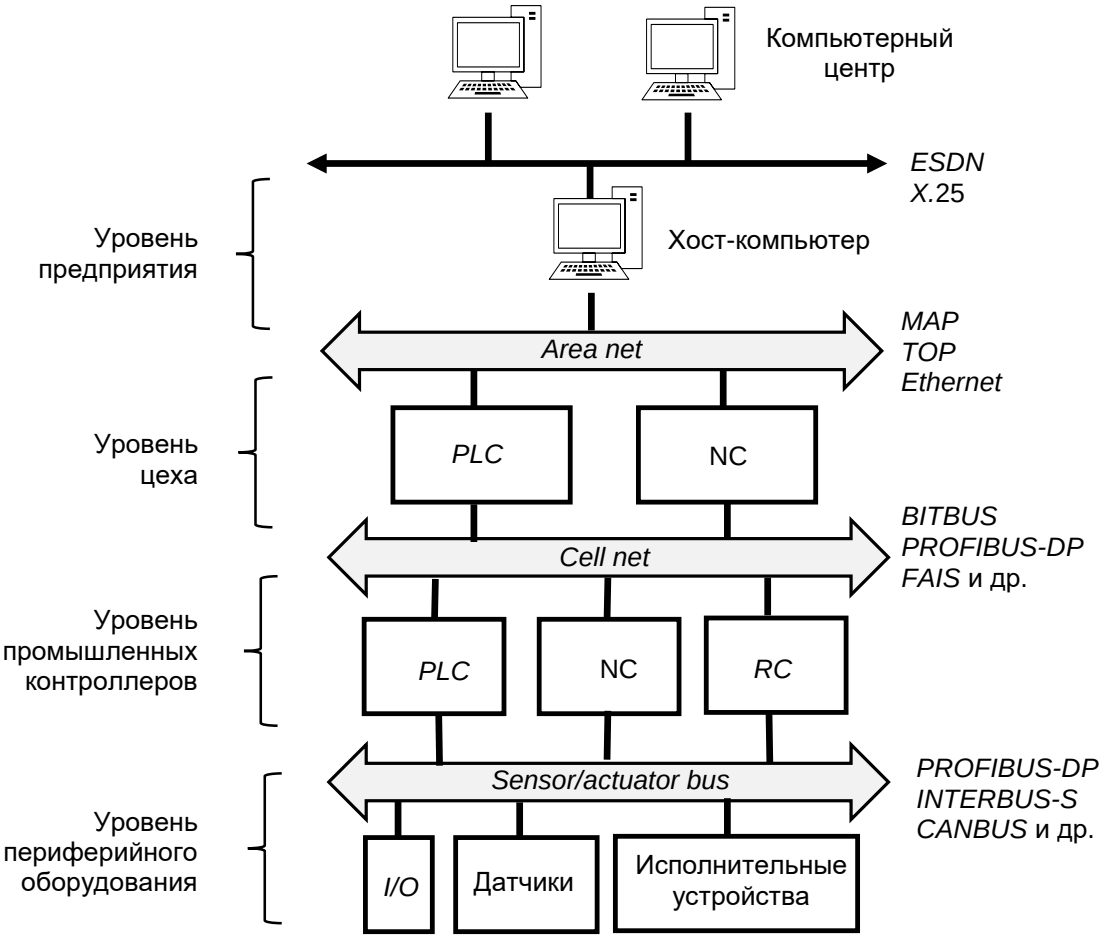


Рис. 17.9. Обобщенная сетевая структура промышленного предприятия

Протокол MODBUS

Протокол *MODBUS* разработан фирмой *Gould Inc*. для построения промышленных распределенных систем управления и работает по принципу *MASTER-SLAVE*, или «ведущий-ведомый». Конфигурация на основе этого протокола предполагает наличие одного *MASTER*-узла и до 247 *SLAVE*-узлов. Только *MASTER* инициирует циклы обмена данными.

Существуют два типа запросов:

1) запрос/ответ (адресуется только один из *SLAVE*-узлов);

2) широковещательная передача (*MASTER* через выставление адреса 0 обращается ко всем остальным узлам сети одновременно без квитирования).

Протокол *MODBUS* описывает фиксированный формат команд, последовательность полей в команде, обработку ошибок и исключительных состояний, коды функций. Для кодирования передаваемых данных используются форматы *ASCII* (*American Standard Code for Information Interchange*) и *RTU* (*Remote Terminal Unit*). Каждый запрос со стороны ведущего узла включает код команды (чтение, запись и т.д.), адрес абонента (адрес 0 используется для широковещательной передачи), размер поля данных, собственно данные или буфер под данные и контрольный *CRC*-код. Функция обслуживания тайм-аута реализована для фиксирования коллизий при приеме/передаче данных.

Протокол CANBUS

CAN (*Control Area Network*) – последовательная магистраль, обеспечивающая увязку в сеть «интеллектуальных» устройств ввода/вывода, датчиков и исполнительных устройств некоторого механизма или даже предприятия.

Протокол *CAN* был предложен компанией *Bosch* для создания сети контроллеров в автомобилях. В настоящее время сети *CAN* активно применяются в самых разных областях (от стиральных машин до космических аппаратов).

Протокол *CAN* определяет только первые два уровня модели *ISO/OSI* – физический и канальный. На основе этого протокола реализовано огромное количество полнофункциональных сетей, таких как *CANOpen, DeviceNet, SDS* и др. Количество узлов промышленных сетей, работающих на основе *CAN*, исчисляется десятками миллионов. Практически у каждого крупного производителя микроконтроллеров есть изделие с *CAN*-интерфейсом.

Широкому распространению *CAN* способствуют его многочисленные достоинства, среди которых:

- невысокая стоимость как самой сети, так и ее разработки;
- высокая степень надежности и живучести сети благодаря развитым механизмам обнаружения ошибок, повтору ошибочных сообщений, самоизоляции неисправных узлов, нечувствительности к электромагнитным помехам;

- простота конфигурирования и масштабирования сети, отсутствие теоретических ограничений на количество узлов;
- поддержка разнотипных физических сред передачи данных от витой пары до оптоволокна и радиоканала;
- эффективная реализация режима реального времени.

Протокол *CAN* обеспечивает возможность нахождения на магистрали нескольких ведущих устройств, обеспечивающих передачу данных в реальном масштабе времени и коррекцию ошибок, высокую помехоустойчивость (рис. 17.10).

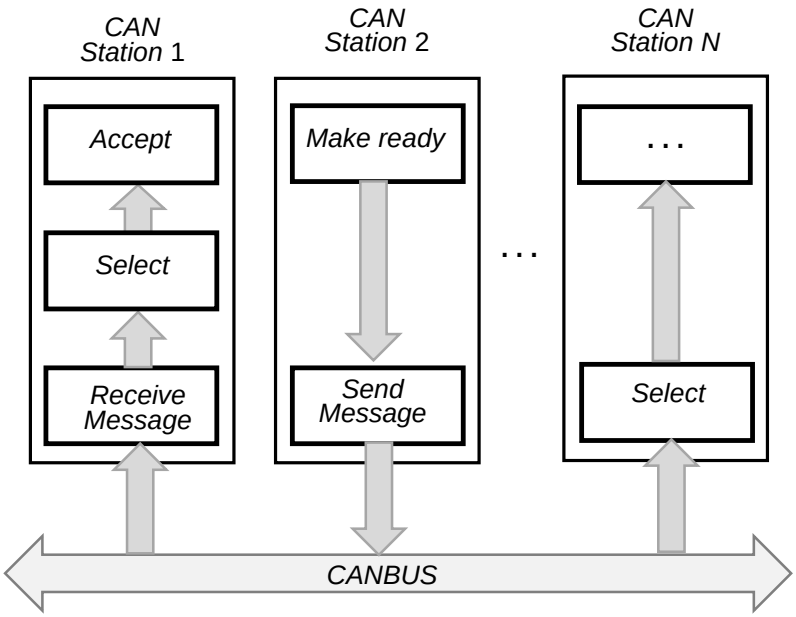


Рис. 17.10. Последовательная магистраль *CAN*

Основные характеристики протокола

Стандарт	*ISO* 11898
Скорость передачи	1 Мб/с (максимум)
Расстояние передачи	1000 м (максимум)
Характер сигнала, линия передачи	Дифференциальное напряжение, скрученная пара
Количество драйверов	64
Количество приемников	64
Схема соединения	Полудуплекс, многоточечная

Скорость передачи здесь задается программно и может быть до 1 Мб/с. Пользователь выбирает скорость, исходя из расстояний, числа абонентов и емкости линий передачи.

Расстояние, м	25	50	100	250	500	1000	2500	5000
Скорость, кб/с	1000	800	500	250	125	50	20	10

Система *CAN* обеспечена большим количеством микросхем, обеспечивающих работу подключенных к магистрали устройств, разработку которых начинала компания *Bosch* для использования в автомобилях, и в настоящее время широко используемых в автоматизации промышленности. Цоколёвка разъема приведена на рис. 17.11.

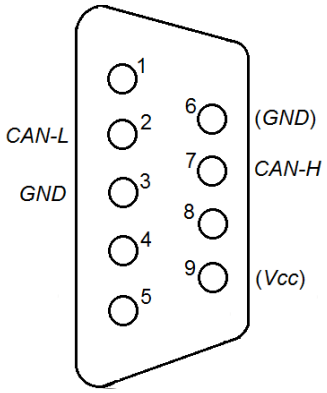


Рис. 17.11. Цоколёвка разъема *CAN*

Максимальное число абонентов, подключенных к данному интерфейсу, фактически определяется нагрузочной способностью применённых приемопередатчиков. Например, при использовании трансивера фирмы *Philips PCA*82*C*250 нагрузочная способность равна 110.

Протокол *CAN* использует оригинальную систему адресации сообщений. Каждое сообщение снабжается идентификатором, который определяет назначение передаваемых данных, но не адрес приемника. Любой приемник может реагировать как на один идентификатор, так и на несколько. На один идентификатор могут реагировать несколько приемников.

Протокол обладает развитой системой обнаружения и сигнализации ошибок. Для этих целей используются поразрядный контроль, прямое заполнение битового потока, проверка пакета сообщения *CRC*-полиномом, контроль формы пакета сообщений, подтверждение правильного приема пакета данных. Хемминговый интервал $d = 6$. Общая вероятность необнаруженной ошибки 4.7x10-11.

Система арбитража протокола *CAN* исключает потерю информации и времени при «столкновениях» на шине.

Интерфейс с применением протокола *CAN* легко адаптируется к физической среде передачи информации. Это может быть дифференциальный сигнал, оптоволокно, просто открытый коллектор и т.п. Несложно сделать гальваническую развязку.

Элементная база, поддерживающая *CAN*, широко выпускается в индустриальном исполнении.

Протокол LonWorks

LonWorks – комплексное управление зданием в режиме реального времени и с высокой безопасностью.

В основе технологии *LonWorks* лежит концепция реализации систем управления при помощи «распределенного интеллекта» – управляющей сети (*Local Operating Networks – LON*), которая имеет минимальное количество уровней иерархии и в которой нет явно выраженного центрального решающего устройства (*Master*). Процессы управления распределяются среди узлов сети, между которыми осуществляются коммуникационные взаимодействия (рис. 17.12). Технология *LonWorks* похожа на нейронные и транспьютерные сети, широко известные специалистам по высокопроизводительным и интеллектуальным вычислительным системам. Так же, как и в этих системах, процессы коммуникации поддерживаются на аппаратном уровне. Делается это при помощи протокола *LonTalk*.

Рис. 17.12. Сеть по протоколу *LonWorks*

Аппаратную основу управляющей сети составляет функционально-ориентированный микроконтроллер *Neuron ChiP* (рис. 17.13).

Рис. 17.13. Микроконтроллер *Neuron Chip*

Разработан язык *Neuron C*, в котором основное внимание уделено вопросам псевдопараллельного программирования, обмену информацией между узлами сети и синхронизации их состояний. В настоящее время во всем мире установлено более 30 млн узлов, функционирующих по технологии *LonWorks*. Все это позволяет говорить (по аналогии с *Internet*, которая представляет собой огромную совокуп-

ность узлов (несколько миллионов), объединенных общим стандартным протоколом взаимодействия – *TCP/IP*) о появлении сетей *Infranet*. *Infranet* – сеть управления окружающей человека инфраструктурой.

Существует возможность управления сетями *Lonworks* с персонального компьютера, мобильного или радиотелефона. Следует отметить, что сетями *LonWorks* можно управлять и удалённо через *Internet*.

Особенности протокола:

- открытость;
- совместимость;
- реализация всех уровней семиуровневой модели *ISO/OSI*;
- разнообразные сетевые структуры и шлюзы к различным сетям;
- событийный механизм обмена сообщениями между узлами;
- сегментация сетей с целью оптимизация трафика.

Протокол *HART*

Протокол *HART* (*Highway Addressable Remote Transducer*), разработанный фирмой *Rosemount Inc*. в середине 1980-х гг., реализует известный стандарт *BELL* 202 *FSK* (*Frequency Shift Keying*) для организации цифровой передачи, основанной на технологии 4 – 20 мА. *HART*-протокол позволяет передавать до 1200 бит/с. *MASTER*-узел дважды в секунду получает все обновленные данные с других узлов.

В *HART*-протоколе реализована схема отношений между узлами сети по принципу *MASTER/SLAVE*, то есть ведомый узел (*SLAVE*) может активизировать среду передачи только по запросу ведомого узла (*MASTER*) (рис. 17.14).

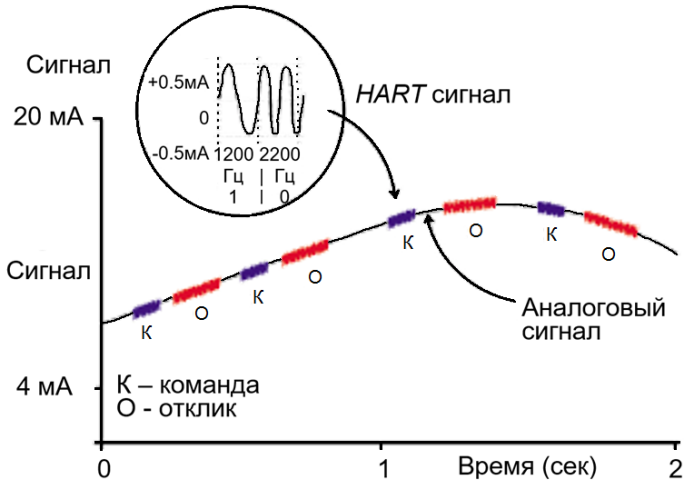


Рис. 17.14. Принцип обмена данными по *HART*-протоколу

В *HART*-сети может присутствовать до двух *MASTER*-узлов (обычно один). Второй *MASTER*, как правило, освобожден от поддержания циклов передачи и занят под связь с какой-либо системой контроля/отображения данных.

Стандартная топология организована по принципу «точка-точка» или «звезда». Для передачи данных по сети используются два режима:

- по схеме «запрос-ответ», т.е. асинхронный обмен данными (один цикл укладывается в 500 мс);
- все пассивные узлы непрерывно передают свои данные на *MASTER*-узел (время обновления данных в *MASTER*-узле 250 – 300 мс).

Возможно построение топологии типа «шина» (до 15 узлов), когда несколько узлов подключены на одну витую пару (рис. 17.15).

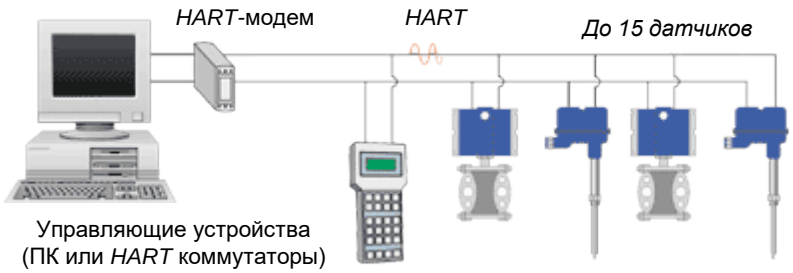


Рис. 17.15. Пример топологии по *HART*-протоколу

Здесь интересна зависимость метода экранирования проводников от длины шины (табл. 17.2).

Табл. 17.2. Зависимость метода экранирования проводников от длины линий в *HART*-сети

Тип проводника	Расстояние, м
Экранированная витая пара	До 1524
Отдельное экранирование проводников в витой паре	От 1524 до 3048

Весь набор команд, реализованных в *HART*-протоколе, условно можно разделить на три группы.

Универсальные команды. Это команды общего назначения и используются на уровне операторских станций: код производителя устрой-

ства в сети, модель, серийный номер, краткое описание устройства, диапазоны ограничений, набор рабочих переменных.

Команды для групп устройств: фиксация значения тока на выходном канале, сброс и т.д.

Команды, зависящие от устройства: старт/стоп, специальные функции калибровки и т.д.

За одну посылку один узел другому может передать до четырех технологических переменных, а каждое *HART*-устройство может иметь до 256 переменных, описывающих его состояние.

Структура информационного байта имеет стандартный формат:

- 1 стартовый бит;
- 8 бит данных;
- 1 бит контроля по нечетности;
- 1 стоповый бит.

Метод контроля корректности передаваемых данных основан на получении подтверждения. В США *HART*-сообщения можно свободно передавать по телефонным линиям. В Европе это не разрешено – необходимо иметь выделенный телефонный канал.

Протокол *AS-Interface*

Основная задача этой сети – связать в единую информационную структуру устройства самого нижнего уровня распределенной системы автоматизации, а именно: датчики и разнообразные исполнительные механизмы, имеющие соответствующий сетевой интерфейс. Название описываемой сети раскрывает ее назначение: *Actuator Sensor Interface (ASI)* – интерфейс с датчиками и исполнительными механизмами.

Впервые *ASI*-протокол вышел на рынок в конце 1989 г. и уже сегодня поддержан рядом известных фирм: *IBM, Limberg, Siemens, Pepperl&Fuchs, Allen-Bradley*. Существует и одноименная ассоциация по поддержке сети *ASI*.

Тенденция в построении распределенных систем автоматизации имеет явное стремление использовать технологии сквозного сетевого доступа. Системе необходимо увязывать в сеть не только контроллеры, но уже желательно и датчики при удовлетворении всем современным требованиям по надежности и открытости, предъявляемым к любой промышленной сети.

Сеть *ASI* эти задачи решает. С ее помощью можно строить системы, в которых датчики и контроллеры связаны одной сетью. Причем *ASI* имеет шлюзы в другие промышленные сети: *Profibus*, *Interbus-S* и др. (рис. 17.16).

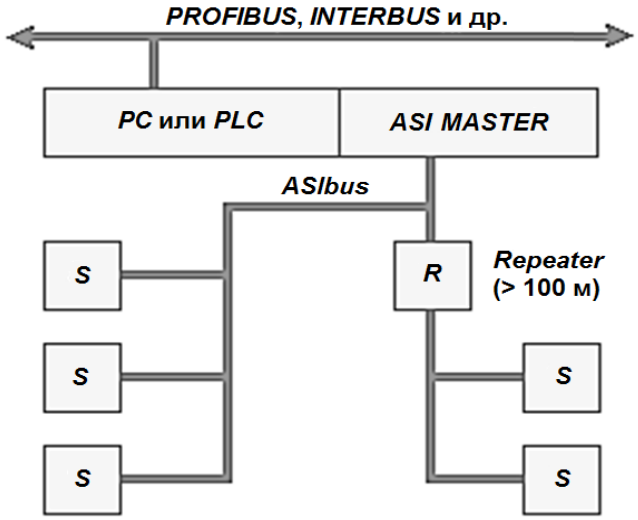
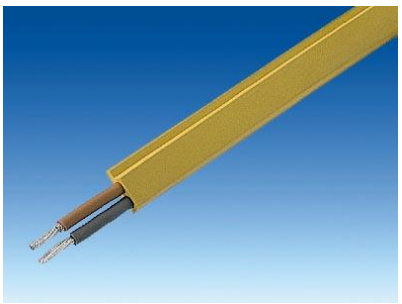


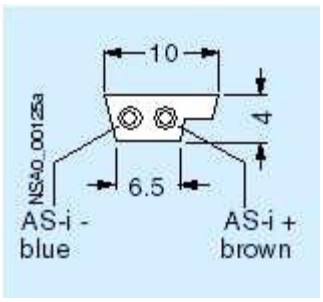
Рис. 17.16. Пример комбинированной сети

Каждый узел *ASI*-сети должен иметь специальный интерфейсный кристалл с поддержкой *ASI*-протокола.

ASI-интерфейс позволяет передавать как данные, так и питающую нагрузку к узлам сети, поскольку существует большое число фотоэлектрических и индуктивных датчиков.

В качестве среды передачи используется пара обычных проводников. Скорость передачи ограничена до 167 кБод. Сегодня появился специальный *ASI*-кабель, в котором оба проводника упакованы в специальную мягкую резиновую оболочку, которая делает этот кабель гибким и устойчивым к многократным изгибам (рис. 17.17, *а*).





а) *б)*

Рис. 17.17. *ASI*-кабель: *а* – внешний вид; *б* – сечение кабеля

Кабель используется для подсоединения датчиков, устанавливаемых на подвижных частях механизмов.

Для кодирования данных используется известный манчестерский код, в котором «0» и «1» кодируются по восходящему и нисходящему фронту сигнала. Такой тип кодирования снижает влияние на *ASI*-кабель внешних возмущений.

Протокол *Profibus*

Profibus (*Process Fieldbus*) появился на свет благодаря усилиям группы немецких компаний: *Bosch, Siemens* и *Klockner-Moller*.

В его задачи входит:

- организация связи с устройствами, гарантирующими быстрый ответ;
- создание простой и экономичной системы передачи данных, основанной на стандартах;
- реализация интерфейса между уровнями 2 и 7 *OSI*-модели.

Стандарт протокола описывает уровни 1, 2 и 7 *OSI*-модели (физический уровень, уровень передачи данных и прикладной уровень). В *Profibus* используется гибридный метод доступа в структуре *MASTER/SLAVE* и децентрализованная процедура передачи маркера. Сеть может состоять из 122 узлов, из которых 32 могут быть *MASTER*-узлами. Адрес 0 зарезервирован для режима широкого вещания («*broadcast*»). Общая схема *Profibus*-сети представлена на рис. 17.18.

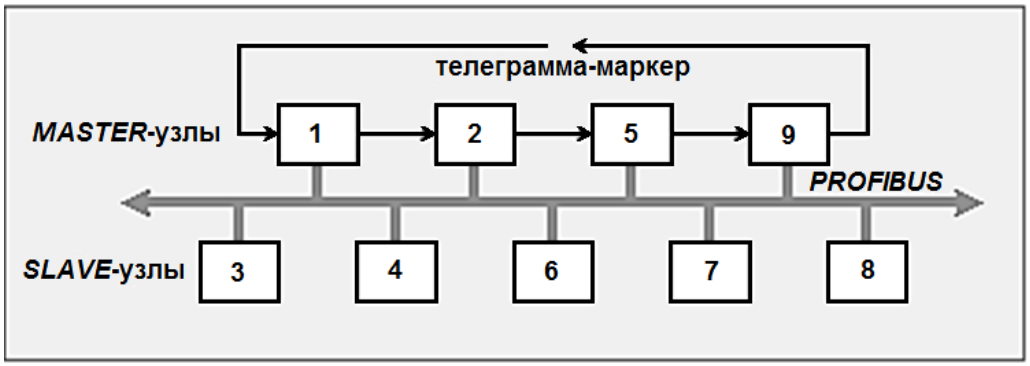


Рис. 17.18. Принцип работы сети *Profibus*

Сегодня, говоря о *Profibus*, необходимо иметь в виду, что под этим общим названием понимается совокупность трех различных, но совместимых протоколов: *Profibus-FMS*, *Profibus-DP* и *Profibus-PA* (рис. 17.19).

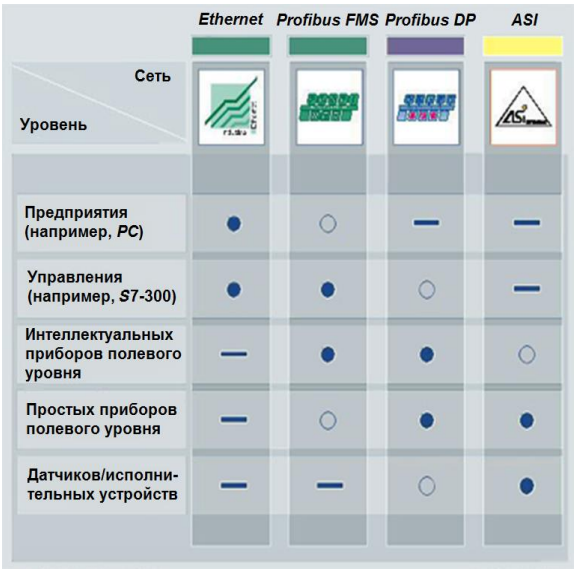


Рис. 17.19. Система протоколов *Profibus*

Протокол *Profibus-FMS* предназначен в основном для связи программируемых контроллеров друг с другом и станциями оператора. Он используется в тех областях, где высокая степень функциональности более важна, чем быстрое время реакции системы.

Очень часто используется комбинированный режим работы устройств *Profibus-FMS* и *Profibus-DP*, в этом случае между мастерами и ведомыми устройствами используется протокол *DP*, а между самими мастерами протокол *FMS*.

Протокол *Profibus-DP* (*Decentralized PerIPheral* – распределённая периферия) ориентирован на обеспечение скоростного обмена данными между:

- системами автоматизации (ведущими *DP*-устройствами),
- устройствами распределённого ввода-вывода (ведомыми *DP*-устройствами).

Протокол характеризуется минимальным временем реакции и высокой стойкостью к воздействию внешних электромагнитных полей. Оптимизирован для высокоскоростных и недорогих систем. Эта версия сети была спроектирована специально для связи между автоматизированными системами управления и распределенной периферией. Электрически близка к *RS*-485, но сетевые карты используют двухпортовую рефлективную память, что позволяет устройствам обмениваться данными без загрузки процессора контроллера.

Протокол *Profibus-PA* (англ. *Process Automation* – автоматизация процесса) – протокол обмена данными с оборудованием полевого уровня, расположенным в обычных или взрывоопасных зонах. Прото-

кол отвечает требованиям международного стандарта *IEC* 61158-2. Позволяет подключать датчики и приводы на одну линейную или кольцевую шину.

В настоящее время применение протокола *Profibus* сокращается, в связи с переходом к промышленным *Ethernet* и *Profinet*. Однако спецификации *FMS* стали частью стандарта *Foundation Fieldbus* и используются в нём. Тем не менее в настоящее время заметна тенденция в динамическом развитии семейства протоколов *Profibus*. К тому же на его основе готовится проект так называемого европейского стандарта промышленной сети, который имеет кодовое название *EN*50170.

Ethernet уже давно завоевал себе прочное лидирующее место на уровне управления производством сети. Решения на базе *Ethernet* практически вытеснили все остальные из офисных распределенных систем, и сегодня *Ethernet* является основным средством обмена в локальных сетях. В последнее время *Ethernet* стал активно проникать и в комплексы управления производственными процессами. Появился целый ряд аппаратных средств (коммутаторов и концентраторов), выполненных в соответствии с требованиями промышленных условий эксплуатации.

Использование *Ethernet* как физической среды передачи данных приводит к использованию хорошо адресуемых логических протоколов. Уже сейчас большинство устройств поддерживают протокол *TCP/IP*. Это позволяет легко интегрировать локальные системы управления технологическими процессами в сети любого масштаба, включая глобальную сеть *Internet*. Отличительные особенности сети *Ethernet*:

- возможность применения открытых сетевых решений;
- общепризнанный мировой стандарт организации промышленной связи;
- основа для применения информационных технологий в АСУТП;
- поддержка *Web*-функций, функций электронной почты, *WAN*-связи;
- простое и быстрое подключение сетевых компонентов;
- высокая гибкость (сети могут расширяться без их остановки);
- высокая надежность, достигаемая резервированием топологий;
- возможность применения в офисных и промышленных условиях;
- использование оборудования множества производителей;
- возможность помехоустойчивой передачи аналогового сигнала на относительно большие расстояния.

Вопросы к компьютерному тестированию

1. В каком из вариантов организации доступа к ресурсам ЛВС сетевой операционной системой не предусматривается использование сервера?
2. На каких уровнях модели *OSI* работают сети *Novell Net Ware*?
3. В каком из двух вариантов топологий локальной вычислительной сети *Net Ware* фирмы *Novell* используется в качестве физической среды тонкий коаксиальный кабель?
4. В каком из двух вариантов топологий локальной вычислительной сети *Net Ware* фирмы *Novell* используется в качестве физической среды витая пара?
5. Что является основными программными компонентами сети *Net Ware*?
6. Каким образом пользователь регистрируется в сети *Net Ware* фирмы *Novell*?
7. Каким образом осуществляется работа бездисковых рабочих станций в сети *Net Ware*?
8. Какова суть доменной модели, используемой в сети на базе *Windows NT Server*?
9. Каков механизм взаимодействия при использовании доменной модели в сети на базе *Windows NT Server*?
10. Какие модели установления доверительных отношений используют в сети на базе *Windows NT Server*?
11. Какие типы учетных записей, содержащих информацию о пользователе, используют в сети на базе *Windows NT Server*?
12. Для чего предназначены структурированные ЛВС с использованием асимметричных *VLAN*-технологий?
13. Как называется метод, используемый сетями на базе *Windows NT Server*, упрощающий централизованное управление сетью и позволяющий использовать *Windows Server* 2000 в качестве сетевой операционной системы предприятия любого масштаба?
14. Что является основной целью разбиения сети на несколько *VLAN*?
15. Какие коммутаторы используются в *VLAN*, каково их назначение?
16. Какие коммутаторы формируют единую производительную информационную магистраль предприятия?

17. Какие коммутаторы служат для увеличения количества портов, требуемых для подключения ПК пользователей?
18. Сколько и какие *VLAN* необходимо создать для организации доступа к общему ресурсу двух потребителей, исключая трафик между ними?
19. В какой из основных архитектур промышленных сетей взаимодействие осуществляется по принципу «запрос – ответ»?
20. Какая из основных архитектур промышленных сетей использует протокол *Profibus* и применяется обычно на нижнем уровне автоматизации?
21. Какая из основных архитектур промышленных сетей применяется для периодического обмена данными с большой интенсивностью?
22. Как называют уровень промышленных сетей, где решают задачи по управлению процессом производства?
23. Как называют уровень промышленных сетей, задачи которого сводятся к опросу датчиков и управлению работой разнообразных исполнительных механизмов?
24. По какому принципу работает протокол промышленных сетей *Modbus*?
25. Какой из протоколов промышленных сетей обеспечивает увязку в сеть «интеллектуальных» устройств ввода/вывода, датчиков и исполнительных устройств?
26. Какая концепция лежит в основе технологии промышленных сетей *LonWorks*?
27. В каком из протоколов промышленных сетей реализован стандарт *BELL FSK* для организации цифровой передачи?
28. Какой из известных кодов используется для кодирования данных в протоколе сети *ASI*?
29. В каком из протоколов промышленных сетей используется гибридный метод доступа в структуре *MASTER/SLAVE* и децентрализованная процедура передачи маркера?
30. Какие из промышленных сетей поддерживают широко распространенный протокол *TCP/IP*?

Глава 18

ГЛОБАЛЬНАЯ СЕТЬ *INTERNET*

Рассматриваемые вопросы:

18.1. Введение в *Internet.*
18.2. Работа со службами *Internet.*
18.2.1. Терминальный режим.
18.2.2. Электронная почта.
18.2.3. Списки рассылки.
18.2.4. Служба телеконференций.
18.2.5. Служба *World Wide Web.*
18.2.6. Служба имен доменов.
18.2.7. Служба передачи файлов (*FTP*).
18.2.8. Служба *Internet Relay Chat.*
18.2.9. Служба *ICQ.*
18.2.10. Облачные технологии.
18.3. Глобальная сеть *Internet*-2.

18.1. Введение в *Internet*

Интерне́т (*Internet,* Всемирная сеть, Глобальная сеть) – всемирная система объединённых компьютерных сетей для хранения и передачи информации. Построена на базе стека протоколов *TCP*/*IP*. На основе *Internet* работает Всемирная паутина (*World Wide Web, WWW*) и множество других систем передачи данных.

Впервые сеть национального масштаба была создана в конце 1960-х гг. на средства Агентства перспективных разработок министерства обороны США. Она получила название *ARPANET*. Эта сеть связывала несколько крупных научных, исследовательских и образовательных центров. Ее основной задачей была координация групп коллективов, работающих над едиными научно-техническими проектами, а основным назначением стал обмен электронной почтой файлами с научной и проектно-конструкторской документацией.

Сеть *ARPANET* заработала в 1969 г. Немногочисленные узлы, входившие в нее в то время, были связаны выделенными линиями. Прием и передача информации обеспечивались программами, работающими на узловых компьютерах. Сеть постепенно расширялась за счет подключения новых узлов, а к началу 1980-х гг. на базе наиболее крупных узлов были созданы свои региональные сети, воссоздающие общую архитектуру *ARPANET* на более низком уровне (в региональном или локальном масштабе).

Днем рождения *Internet* в современном понимании этого слова стала дата стандартизации протокола связи *TCP*/*IP*, лежащего в основе Всемирной сети по нынешний день.

Из вышеизложенного известно, что *TCP*/*IP* – это не один сетевой протокол, а несколько протоколов, лежащих на разных уровнях сетевой модели *OSI* (это так называемый стек протоколов). Из них протокол *TCP* – протокол транспортного уровня. Он управляет тем, как происходит передача информации. Согласно этому протоколу отправляемые данные «нарезаются» на небольшие пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем были данные, необходимые для правильной сборки документа на компьютере получателя.

Протокол *IP* (*Internet Protocol*) – адресный. Он принадлежит сетевому уровню и определяет, куда происходит передача. Суть его состоит в том, что у каждого участника Всемирной сети должен быть свой уникальный адрес (*IP*-адрес). Без этого нельзя говорить о точной доставке *TCP*-пакетов на нужное рабочее место. Этот адрес выражается очень просто – четырьмя байтами, например: 191.38.46.11.

Поскольку один байт содержит до 256 различных значений, то теоретически с помощью четырех байтов можно выразить более четырех миллиардов уникальных *IP*-адресов (256^4 за вычетом некоторого количества адресов, используемых в качестве служебных). На практике же из-за особенностей адресации к некоторым типам локальных сетей количество возможных адресов составляет порядка двух миллиардов, но и это по современным меркам достаточно большая величина.

18.2. Работа со службами *Internet*

Когда говорят о работе в *Internet* или о его использовании, то на самом деле речь идет не об *Internet* в целом, а только об одной или

нескольких из его многочисленных служб. В зависимости от конкретных целей и задач клиенты сети используют те службы, которые им необходимы.

Разные службы имеют разные протоколы. Они называются прикладными протоколами. Их соблюдение обеспечивается и поддерживается работой специальных программ.

Чтобы воспользоваться какой-то из служб *Internet*, необходимо установить на компьютере программу, способную работать по протоколу данной службы. Такие программы называют *клиентскими*, или просто *клиентами*.

Так, например, для передачи файлов в *Internet* используется специальный прикладной протокол *FTP* (*File Transfer Protocol*). Соответственно, чтобы получить из *Internet* файл, необходимо (рис. 18.1):

- иметь на компьютере программу, являющуюся клиентом *FTP* (*FTP*-клиент);
- установить связь с сервером, предоставляющим услуги *FTP* (*FTP*-сервером).

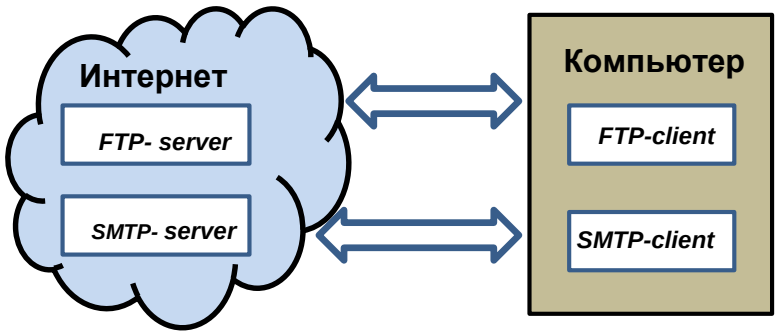


Рис. 18.1. Работа со службами *Internet*

Другой пример: чтобы воспользоваться электронной почтой, необходимо соблюсти протоколы отправки и получения сообщений. Для этого надо:

- иметь программу (почтовый клиент);
- установить связь с почтовым сервером.

Так же обстоит дело и с другими службами.

К основным службам сети *Internet* относят:

- *World Wide Web* – Всемирная паутина – служба поиска и просмотра гипертекстовых документов, включающих в себя графику, звук и видео.

- *E-mail* – электронная почта – служба передачи электронных сообщений по протоколам *SMTP* (отправка), *POP*3 (прием).
- *Usenet, News* – телеконференции, группы новостей – разновидность сетевой газеты или доски объявлений.
- *FTP* – служба передачи файлов.
- *ICQ* – служба для общения в реальном времени с помощью клавиатуры.
- *Telnet* – служба удаленного доступа к компьютерам.
- *Gopher* – служба доступа к информации с помощью иерархических каталогов.

18.2.1. Терминальный режим

Исторически одной из ранних является служба *удаленного управления* компьютером *Telnet*. Подключившись к удаленному компьютеру по протоколу этой службы, можно управлять его работой. Такое управление еще называют *консольным*, или *терминальным*.

В прошлом эту службу широко использовали для проведения сложных математических расчетов на удаленных вычислительных центрах. Так, например, если для очень сложных вычислений на персональном компьютере требовались недели непрерывной работы, а на удаленной супер-ЭВМ всего несколько минут, то персональный компьютер применяли для удаленного ввода данных в ЭВМ и для приема полученных результатов.

В наши дни в связи с быстрым увеличением мощности персональных компьютеров необходимость в подобной услуге сократилась, но тем не менее службы *Telnet* в *Internet* продолжают существовать. Часто протоколы *Telnet* применяют для дистанционного управления техническими объектами, например, телескопами, видеокамерами, промышленными роботами.

Каждый сервер (программное обеспечение), предоставляющий *Telnet*-услуги, обычно предлагает свое клиентское приложение. Его надо получить по сети, установить на своем компьютере, подключиться к серверу и работать с удаленным оборудованием. Простейший клиент *Telnet* входит в состав операционной системы *Windows* (файл *telnet.exe*).

18.2.2. Электронная почта

Электронная почта (E-mail) является одной из наиболее ранних служб. Ее обеспечением в *Internet* занимаются специальные почтовые серверы.

Почтовые серверы получают сообщения от клиентов и пересылают их по цепочке к почтовым серверам *адресатов*, где эти сообщения накапливаются. При установлении соединения между адресатом и его почтовым сервером происходит автоматическая передача сообщений, поступивших на компьютер адресата.

Почтовая служба основана на *двух прикладных протоколах*: *SMTP* и *POP*3. По первому происходит отправка корреспонденции с компьютера на сервер, а по второму – прием поступивших сообщений.

Существует большое разнообразие клиентских почтовых программ. К ним относится, например программа *Microsoft Outlook Express*, входящая в состав операционной системы *Windows* как стандартная. Более мощная программа, интегрирующая в себе кроме поддержки электронной почты и другие средства делопроизводства, *Microsoft Outlook* 2000, входит в состав известного пакета *Microsoft Office* 2000. Из специализированных почтовых программ хорошую популярность имеют программы *The Bat! и Eudora Pro*.

18.2.3. Списки рассылки

Обычная электронная почта предполагает наличие двух партнеров по переписке. Если же партнеров нет, то достаточно большой поток почтовой информации в свой адрес можно обеспечить, подписавшись на списки *рассылки (Mail list)*. Это специальные *тематические серверы*, собирающие информацию по определенным темам и переправляющие ее подписчикам в виде сообщений электронной почты.

Темами списков рассылки может быть что угодно, например вопросы, связанные с изучением иностранных языков, научно-технические обзоры, презентация новых программных и аппаратных средств вычислительной техники.

Большинство телекомпаний создают списки рассылки на своих узлах, через которые рассылают клиентам аннотированные обзоры телепрограмм.

18.2.4. Служба телеконференций

Служба телеконференций *(Usenet)* похожа на циркулярную рассылку электронной почты, в ходе которой одно сообщение отправляется не одному корреспонденту, а *большой группе* (такие группы называются телеконференциями, или группами новостей).

Сообщения, направленные на сервер группы новостей, отправляются с него на все серверы, с которыми он связан, если на них данного сообщения еще нет. Далее процесс повторяется. Характер распространения каждого отдельного сообщения напоминает лесной пожар.

На каждом из серверов поступившее сообщение хранится ограниченное время (обычно неделю), и все желающие могут в течение этого времени с ним ознакомиться. Распространяясь во все стороны, менее чем за сутки сообщения охватывают весь земной шар. Далее распространение затухает, поскольку на сервер, который уже имеет данное сообщение, повторная передача производиться не может.

Ежедневно в мире создается порядка *миллиона сообщений* для групп новостей. Выбрать в этом массиве действительно полезную информацию практически невозможно. Поэтому вся система телеконференций разбита на *тематические группы*. Сегодня в мире насчитывают порядка 50 000 тематических групп новостей. Они охватывают большинство тем, интересующих массы.

Основной прием использования групп новостей состоит в том, чтобы задать вопрос, обращаясь ко всему миру, и получить ответ или совет от тех, кто с этим вопросом уже разобрался. При этом важно следить за тем, чтобы содержание вопроса соответствовало теме данной телеконференции.

Многие квалифицированные специалисты мира регулярно просматривают сообщения телеконференций, проходящие в группах, касающихся их сферы деятельности. Такой просмотр называется *мониторингом информации*. Регулярный мониторинг позволяет специалистам точно знать, что нового происходит в мире по их специальности, какие проблемы беспокоят большие массы людей и на что надо обратить особое внимание в своей работе.

В современных промышленных и проектно-конструкторских организациях считается хорошим тоном, если специалисты высшего эшелона периодически (один-два раза в месяц) отвечают через систему телеконференций на типовые вопросы пользователей своей продукции.

При отправке сообщений в телеконференции принято указывать свой адрес электронной почты для обратной связи.

Огромный объем сообщений в группах новостей значительно затрудняет их целенаправленный мониторинг, поэтому в некоторых группах производится предварительный «отсев» бесполезной информации (в частности, рекламной), не относящейся к теме конференции. Такие конференции называют *модерируемыми*. В качестве *модератора* может выступать не только человек, но и программа, фильтрующая сообщения по определенным ключевым словам. В последнем случае говорят об *автоматической модерации*.

Для работы со службой телеконференций существуют специальные клиентские программы. Так, например, приложение *Microsoft Outlook Express*, указанное выше как почтовый клиент, позволяет работать также и со службой телеконференций. Для начала работы надо настроить программу на взаимодействие с сервером групп новостей, оформить «подписку» на определенные группы и периодически, как и на электронную почту, получать все сообщения, проходящие по теме этой группы. В данном случае слово «подписка» не предполагает со стороны клиента никаких обязательств или платежей – это просто указание серверу о том, что сообщения по указанным темам надо доставлять, а по прочим – нет. Отменить подписку или изменить ее состав можно в любой удобный момент.

18.2.5. Служба World Wide Web

Безусловно, это самая популярная служба современного *Internet*. Ее нередко отождествляют с *Internet*, хотя на самом деле это лишь одна из его многочисленных служб.

World Wide Web (WWW) – это единое информационное пространство, состоящее из сотен миллионов взаимосвязанных электронных документов, хранящихся на *Web*-серверах. Отдельные документы, составляющие пространство *Web*, называют *Web-страницами*. Группы тематически объединенных *Web*-страниц называют *Web-узлами* (жаргонный термин – *Web*-сайт или просто сайт). Один физический *Web*-сервер может содержать достаточно много *Web*-узлов, каждому из которых, как правило, отводится отдельный каталог на жестком диске сервера.

От обычных текстовых документов *Web*-страницы отличаются тем, что они оформлены без привязки к конкретному носителю. Например, оформление документа, напечатанного на бумаге, привязано к параметрам печатного листа, который имеет определенную ширину, высоту и размеры полей. Электронные *Web*-документы предназначены для просмотра на экране компьютера, причем заранее не известно, на каком. Неизвестны ни размеры экрана, ни параметры цветового и графического разрешения, неизвестна даже операционная система, с которой работает компьютер клиента. Поэтому *Web*-документы не могут иметь «жесткого» форматирования. Оформление выполняется непосредственно во время их воспроизведения на компьютере клиента и происходит оно в соответствии с настройками программы, выполняющей просмотр.

Программы для просмотра *Web*-страниц называют *браузерами*. В литературе также можно встретить «неустоявшиеся» термины «*браузер*» и «*обозреватель*». Во всех случаях речь идет о некотором средстве просмотра *Web*-документов.

Браузер выполняет отображение документа на экране, руководствуясь командами, которые автор документа внедрил в его текст. Такие команды называются *тегами*. От обычного текста они отличаются тем, что заключены в угловые скобки. Большинство тегов используются парами: открывающий тег и закрывающий. Закрывающий тег начинается с символа «/».

<*CENTER*> Этот текст должен выравниваться по центру экрана </*CENTER*>

<*LEFT*> Этот текст выравнивается по левой границе экрана </*LEFT*>

<*RIGHT*> Этот текст выравнивается по правой границе экрана </*RIGHT*>

Сложные теги имеют кроме ключевого слова дополнительные атрибуты и параметры, детализирующие способ их применения. Правила записи тегов содержатся в спецификации особого языка разметки, близкого к языкам программирования. Он называется *языком разметки гипертекста – HTML* (*HyperText Markup Language*).

Web-документ представляет собой обычный текстовый документ, размеченный тегами *HTML*. Такие документы также называют *HTML*-документами, или документами в формате *HTML*.

При отображении *HTML*-документа на экране с помощью браузера теги не показываются, и мы видим только текст, составляющий документ. Однако оформление этого текста (выравнивание, цвет, размер и начертание шрифта и прочее) выполняется в соответствии с тем, какие теги имплантированы в текст документа.

Существуют *специальные теги* для внедрения графических и мультимедийных объектов (звук, музыка, видеоклипы). Встретив такой тег, обозреватель делает запрос к серверу на доставку файла, связанного с тегом, и воспроизводит его в соответствии с заданными атрибутами и параметрами тега – мы видим иллюстрацию или слышим звук.

В последние годы в *Web*-документах находят широкое применение так называемые *активные компоненты*. Это тоже объекты, но они содержат не только текстовые, графические и мультимедийные данные, но и программный код, то есть могут не просто отображаться на компьютере клиента, но и выполнять на нем работу по заложенной в них программе.

Наиболее важной чертой *Web*-страниц, реализуемой с помощью тегов *HTML*, являются *гипертекстовые ссылки*. С любым фрагментом текста или, например, с рисунком с помощью тегов можно связать иной *Web*-документ, то есть установить гиперссылку. В этом случае при щелчке по левой кнопке мыши на тексте или рисунке, являющемся гиперссылкой, отправляется запрос на доставку нового документа. Этот документ, в свою очередь, тоже может иметь гиперссылки на другие документы.

Совокупность огромного числа гипертекстовых электронных документов, хранящихся на серверах *WWW*, образует *гиперпространство документов*, между которыми возможно перемещение.

Произвольное перемещение между документами в *Web*-пространстве называют *Web-серфингом* (с целью ознакомления с информацией).

Целенаправленное перемещение между *Web*-документами называют *Web-навигацией* (выполняется с целью поиска нужной информации).

Гипертекстовая связь в пространстве *WWW* не могла бы существовать, если бы каждый документ в этом пространстве не обладал своим уникальным адресом.

Каждый файл одного локального компьютера обладает уникальным полным именем, в которое входит собственное имя файла (включая расширение имени) и путь доступа к файлу, начиная от имени устройства, на котором он хранится.

Адрес любого файла во Всемирной сети определяется унифицированным указателем ресурса – *URL*.

Адрес URL состоит из трех частей.

1. Указание службы, которая осуществляет доступ к данному ресурсу (обычно обозначается именем прикладного протокола, соответствующего данной службе). Так, например, для службы *WWW* прикладным является протокол *HTTP* (*HyperText Transfer Protocol* – протокол передачи гипертекста). После имени протокола ставится двоеточие (:) и два знака «/» (косая черта): *http://...*

2. Указание доменного имени компьютера (сервера), на котором хранится данный ресурс: *http://wmw.abcde.com...*

3. Указания полного пути доступа к файлу на данном компьютере. В качестве разделителя используется символ «/» (косая черта): *http://WWW.abcde.com/Fllea/New/abcdefg.zIP*

При записи *URL*-адреса важно точно соблюдать регистр символов. В отличие от правил работы в *MS-DOS* и *Windows* в *Internet* строчные и прописные символы считаются разными.

Именно в форме *URL* и связывают адрес ресурса с гипертекстовыми ссылками на *Web*-страницах. При активации гиперссылки браузер посылает запрос для поиска и доставки ресурса, указанного в ссылке. Если по каким-то причинам он не найден, выдается сообщение о том, что ресурс недоступен (возможно, что сервер временно отключен или изменился адрес ресурса).

18.2.6. Служба имен доменов

Адрес любого компьютера или любой локальной сети в *Internet* может быть выражен четырьмя байтами, например так: 195.28.132.97.

Каждый компьютер имеет уникальное доменное имя, например такое: *WWW.abcdef.com.*

Это просто две разные формы записи адреса одного и того же сетевого компьютера. Человеку неудобно работать с числовым представлением *IP*-адреса, зато доменное имя запоминается легко, особенно если учесть, что, как правило, это имя имеет содержание.

Например, *Web*-сервер компании *Microsoft* имеет имя *WWW. microsoft.com*, а *Web*-сервер компании «Космос ТВ» имеет имя *WWW. kosmostv.ru* (суффикс *.ru* в конце имени говорит о том, что сервер компании принадлежит российскому сектору *Internet*).

С другой стороны, автоматическая работа серверов сети организована с использованием четырехзначного числового адреса. Благодаря ему промежуточные серверы могут осуществлять передачу запросов и ответов в нужном направлении.

Поэтому необходим перевод доменных имен в связанные с ними *IP*-адреса. Этим и занимаются серверы службы имен доменов *(DNS)*. Запрос на получение одной из страниц сервера *WWW.abcde.com* сначала обрабатывается сервером *DNS*, и далее он направляется по *IP*-адресу, а не по доменному имени.

База данных *DNS* имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных *DNS* управляется центром *Internet Network Information Center*. Домены верхнего уровня условно можно разделить на «*организационные*» и «*географические*». В табл. 18.1 и 18.2 приведены примеры таких доменов.

Табл. 18.1. Примеры «*организационных*» доменов

Обозначение	Назначение	Обозначение	Назначение
com	*commercial* (коммерческие)	*mil*	*military* (военные)
edu	*educational* (образовательные)	*net*	*network* (организации, обеспечивающие работу сети)
gov	*goverment* (правительственные)	*org*	*organization* (некоммерческие организации)

Каждая страна (государство) имеет свой географический домен из двух букв.

Табл. 18.2. Примеры «*географических*» доменов

Обозначение	Государство	Обозначение	Государство
ae	*United Arab Emirates* (Объединенные Арабские Эмираты)	*au*	*Australia* (Австралия)
be	*Belgium* (Бельгия)	*br*	*Brazil* (Бразилия)
by	*Belarus* (Белоруссия)	*ca*	*Canada* (Канада)
ch	*Switzerland* (Швейцария)	*cz*	*Czech Republic* (Чехия)
de	*Germany* (Германия)	*dk*	*Denmark* (Дания)
do	*DominiCAN Republic* (Доминиканская Республика)	*ee*	*Estonia* (Эстония)
es	*Spain* (Испания)	*fi*	*Finland* (Финляндия)
fr	*France* (Франция)	*hu*	*Hungary* (Венгрия)
il	*Israel* (Израиль)	*in*	*India* (Индия)
jp	*Japan* (Япония)	*kg*	*Kyrgyzstan* (Кыргызстан)
kr	*South Korea* (Южная Корея)	*kz*	*Kazakhstan* (Казахстан)
lt	*Lithuania* (Литва)	*lv*	*Latvia* (Латвия)
mx	*Mexico* (Мексика)	*nl*	*Netherlands* (Нидерланды)
no	*Norway* (Норвегия)	*nz*	*New Zealand* (Новая Зеландия)
pl	*Poland* (Польша)	*ro*	*Romania* (Румыния)
ru	*Russia* (Россия)	*si*	*Slovenia* (Словения)
sk	*Slovak Republic* (Словакия)	*su*	*Soviet Union* (Советский Союз – поддерживается, но не распределяется)
ua	*Ukraine* (Украина)	*uk*	*United Kingdom* (Соединенное Королевство Великобритании и Северной Ирландии)
yu	*Yugoslavia* (Югославия)	*za*	*South Africa* (Южная Африка)

В доменах государств также имеются «*организационные*» и «*географические*» домены нижнего уровня. «*Организационные*» в большинстве своем повторяют структуру «*организационных*» доменов верхнего уровня. «*Географические*» выделяются городам, областям и тому подобным территориальным образованиям. Непосредственно в тех и других размещаются домены организаций или домены персональных пользователей. Обычно это имя компании, торговая марка или что-нибудь столь же характерное. Для неанглоязычных стран используется транскрипция имен. Часто возникают конфликты, связанные с тем, что одно и то же имя используется несколькими фирмами (зако-

нодательство допускает это для фирм, работающих в разных отраслях); многие люди заранее резервируют имена, могущие стать популярными для последующей продажи их владельцу торговой марки; но это уже касается юридической стороны функционирования *Internet*.

С левого конца доменного имени находятся имена машин. Имена бывают «*собственные*» и «*функциональные*». Имена «*собственные*» каждый придумывает в меру фантазии: машинам присваиваются имена членов семьи, животных, растений, музыкантов и артистов, литературных персонажей.

Имена «*функциональные*» вытекают из функций, выполняемых машиной:

- *WWW – HTTP* (*WWW*) сервер;
- *FTP – FTP* сервер;
- *ns, nss, dns – DNS* (*Name*) сервер;
- *mail – Mail* сервер;
- *relay – Mail Exchanger*;
- *proxy* – соответствующий *Proxy* сервер.

Каждый домен (верхних уровней) *DNS* администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов – уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети *Internet* однозначно определяется своим *полным доменным именем (fully qualified domain name, FQDN)*, которое включает имена всех доменов по направлению от хоста к корню. Пример полного *DNS*-имени – *WWW.zsu.zp.ua*.

В сетях *Windows* используется еще *WINS* (*Window Internet Name Service*) – аналог *DNS*, но с динамическим отслеживанием и без какого-либо масштабирования, определяющий соответствие имен *Windows Network* и *IP*-номеров машин.

18.2.7. Служба передачи файлов (FTP)

Необходимость в передаче файлов возникает, например, при приеме файлов программ, при пересылке крупных документов (например, книг), а также при передаче архивных файлов, в которых запакованы большие объемы информации.

Служба *FTP* имеет свои серверы в мировой сети, на которых хранятся архивы данных. Со стороны клиента для работы с серверами *FTP* может быть установлено специальное программное обеспечение, хотя в большинстве случаев браузеры *WWW* обладают встроенными возможностями для работы и по протоколу *FTP*.

Протокол *FTP* работает одновременно с двумя *TCP*-соединениями между сервером и клиентом. По одному соединению идет передача данных, а второе соединение используется как управляющее.

Протокол *FTP* также предоставляет серверу средства для *идентификации* обратившегося клиента. Этим часто пользуются коммерческие серверы и серверы ограниченного доступа, поставляющие информацию только зарегистрированным клиентам – они выдают запрос на ввод имени пользователя и связанного с ним пароля. Однако существуют и десятки тысяч *FTP*-серверов с анонимным доступом для всех желающих. В этом случае в качестве имени пользователя надо ввести слово: *anonymous*, а в качестве пароля задать адрес электронной почты. В большинстве случаев программы-клиенты *FTP* делают это автоматически.

18.2.8. Служба Internet Relay Chat

Служба *IRC* (*Internet Relay Chat*) предназначена для прямого общения нескольких человек в режиме реального времени. Иногда службу *IRC* называют чат-конференциями, или просто чатом.

В отличие от системы телеконференций, в которой общение между участниками обсуждения темы открыто всему миру, в системе *IRC* общение происходит только в пределах одного канала, в работе которого принимают участие обычно лишь несколько человек. Каждый пользователь может создать собственный канал и пригласить в него участников «беседы» или присоединиться к одному из открытых в данный момент каналов.

Существуют несколько популярных клиентских программ для работы с серверами и сетями, поддерживающими сервис *IRC*. Одна из наиболее популярных – программа *mtRC.exe*.

18.2.9. Служба ICQ

Эта служба предназначена для поиска сетевого *IP*-адреса человека, подключенного в данный момент к *Internet*.

Необходимость в подобной услуге связана с тем, что большинство пользователей не имеют постоянного *IP*-адреса. Название службы является акронимом выражения *I seek you* – я тебя ищу.

Для пользования этой службой надо зарегистрироваться на ее центральном сервере (*http://WWW.icq.com*) и получить персональный идентификационный номер *UIN* (*Universal Internet Number*). Данный номер можно сообщить партнерам по контактам, и тогда служба *ICQ* приобретает характер *Internet*-пейджера. Зная номер *UIN* партнера, но не зная его текущий *IP*-адрес, можно через центральный сервер службы отправить ему сообщение с предложением установить соединение.

Каждый компьютер, подключенный к *Internet*, должен иметь четырехзначный *IP*-адрес. Этот адрес может быть постоянным или динамически временным. Те компьютеры, которые включены в *Internet* на постоянной основе, имеют постоянные *IP*-адреса. Большинство же пользователей подключаются к *Internet* лишь на время сеанса. Им выдается динамический *IP*-адрес, действующий только в течение данного сеанса. Этот адрес выдает тот сервер, через который происходит подключение. В разных сеансах динамический *IP*-адрес может быть различным, причем заранее неизвестно каким.

При каждом подключении к *Internet* программа *ICQ*, установленная на компьютере, определяет текущий *IP*-адрес и сообщает его центральной службе, которая, в свою очередь, оповещает ваших партнеров по контактам. Далее ваши партнеры (если они тоже являются клиентами данной службы) могут установить с вами прямую связь. Программа предоставляет возможность выбора режима связи («готов к контакту»; «прошу не беспокоить, но готов принять срочное сообщение»; «закрыт для контакта» и т.п.). После установления контакта связь происходит в режиме, аналогичном сервису *IRC*.

18.2.10. Облачные технологии

Облачные технологии – это обработка данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как *Internet*-сервис.

Суть облачных технологий заключается в предоставлении пользователям хостинга удаленного доступа к услугам, вычислительным ресурсам и приложениям через *Internet* (рис. 18.2).

Рис. 18.2. Объекты обслуживания облачного сервиса

Хостинг – это услуга по размещению оборудования клиента на территории провайдера, при этом обеспечивается подключение его к каналам связи с высокой пропускной способностью. Эта сфера хостинга развивается в связи с возникшей потребностью в программном обеспечении и цифровых услугах, которыми можно было бы управлять изнутри, но которые были бы при этом более экономичными и эффективными.

Существуют три основные модели обслуживания предоставляемых услуг – это *Software as a Service*, или сокращенно *SaaS*, *Platform as a Service*, или *PaaS*, и *Infrastructure as a Service*, сокращенно *IaaS*. Следует более внимательно рассмотреть все модели обслуживания (рис. 18.3).

Рис. 18.3. Модели обслуживания в облачных технологиях

1. Software as a Service

Программное обеспечение как услуга – эта модель обусловливается следующим. Представитель услуг (провайдер) разрабатывает *Web*-приложение, производит его настройку и дальнейшее управление. Заказчик получает через *Internet* доступ к программному обеспечению. Все затраты на содержание приложения и поддержку его работоспособности лежат на провайдере, а потребитель только оплачивает использование программного обеспечения облачного сервиса.

2. Platform as a Service

Платформа как услуга – предоставление провайдером платформы, на которой могут производиться разработки, развертывание, тестирование *Web*-приложений их поддержки и тому подобные операции. Такие платформы должны обладать определенными характеристиками: инструментами создания; системами управления базами данных; связующим программным обеспечением; средами исполнения языков программирования.

Управление и контроль за физической и виртуальной инфраструктурой облачного сервиса, осуществляемые представителем услуги.

3. Infrastructure as a Service

Инфраструктура как услуга в основном рассчитана на использование предприятиями. Клиенту предлагаются различные инфраструктуры: серверов; хранилищ данных; сетевого оборудования; программного оборудования для управления всеми ресурсами. Основным плюсом данной услуги для пользователя является то, что ему нет нужды приобретать дорогое оборудование, необходимое для выполнения какой-либо задачи. Клиент оплачивает только за то, что ему необходимо в конкретный момент для выполнения определенной задачи.

Существуют четыре модели развертывания (*Deployment Models*) облака, рассмотрим их.

1. Private cloud – частное облако. Данная инфраструктура используется при обслуживании одной организации, но дает возможность включения нескольких потребителей. Управляться такое облако может как самой организацией, так и третьей стороной. Эти инфраструктуры применяются как у потребителя, так и у внешнего провайдера.

2. Public cloud – публичное облако. Такое облако создается доступным для большой группы пользователей. Иногда эти пользователи не связаны между собой общими интересами, но ведут работы в одной

области деятельности. Такие сервисы часто бывают собственностью различных организаций – коммерческих, управленческих, правительственных, научных и т. д. Физически облако принадлежит представителю услуг.

3. Community cloud – общественное облако. Вид облака, которое используется определенным сообществом или организациями, имеющими общие задачи (требований безопасности, миссии, политики и др.). Данная структура может управляться как самим обществом, так и третьей стороной, и существовать как на стороне пользователя, так и у провайдера.

4. Hybrid cloud – гибридное облако. Это сочетание двух или более облачных структур, связанных между собой технологиями (стандартизованными или частными) передачи данных и приложений. Например, пакетная передача данных.

По сравнению с традиционным подходом облачные сервисы позволяют управлять более крупными инфраструктурами, обслуживать различные группы пользователей в пределах одного облака, а также означают полную зависимость от провайдера облачных услуг.

При предоставлении облачного сервиса используется следующий тип оплаты (плата за использование): обычно за единицу измерения времени работы принимается минута или час пользования ресурсами. При оценке объемов данных за единицу измерения принимается мегабайт хранимой информации. В этом случае пользователь оплачивает тот объем ресурсов, который им в реальности использовался в течение определенного времени. Кроме того, облачные технологии предоставляют пользователю возможность при необходимости поднимать или опускать максимальные лимиты выделяемых ресурсов, пользуясь таким образом эластичностью предоставляемого сервиса. Пользователю облачных сервисов нет необходимости заботиться об инфраструктуре, которая обеспечивает работоспособность предоставляемых ему сервисов. Все задачи по настройке, устранению неисправностей, расширению инфраструктуры и прочие берет на себя сервис-провайдер.

Преимущества облачных технологий

1. Пользователь оплачивает услугу только тогда, когда она ему необходима, а самое главное, он платит только за то, что использует.

2. Облачные технологии позволяют экономить на приобретении, поддержке, модернизации ПО и оборудования.
3. Масштабируемость, отказоустойчивость и безопасность – автоматическое выделение и освобождение необходимых ресурсов в зависимости от потребностей приложения. Техническое обслуживание, обновление ПО производит провайдер услуг.
4. Удаленный доступ к данным в облаке – работать можно из любой точки на планете, где есть доступ в сеть *Internet*.

Недостатки облачных технологий

1. Пользователь не является владельцем и не имеет доступа к внутренней облачной инфраструктуре. Сохранность пользовательских данных сильно зависит от компании провайдера.
2. Недостаток, актуальный для российских пользователей: для получения качественных услуг пользователю необходимо иметь надежный и быстрый доступ в сеть *Internet*.
3. Не все данные можно доверить провайдеру в *Internet* не только для хранения, но даже для обработки.
4. Не каждое приложение позволяет сохранить, например на флэш-накопителе, промежуточные этапы обработки информации, а также конечный результат работы, так как онлайновые результаты удобны не всегда.
5. Есть риск, что провайдер онлайновых сервисов однажды не сделает резервную копию данных и они будут утеряны в результате крушения сервера.
6. Доверяя свои данные онлайн-сервису, вы теряете над ними контроль и ограничиваете свою свободу. Пользователь будет не в состоянии изменить какую-то часть своей информации, она будет храниться в условиях, не подвластных ему.

Как пример использования облачных технологий в образовании можно назвать:

1) электронные дневники;
2) журналы;
3) личные кабинеты для учащихся и преподавателей;
4) интерактивную приемную;
5) тематические форумы, где студенты могут обмениваться информацией;

6) поиск информации, где учащиеся могут решать определенные учебные задачи даже в отсутствие педагога или под его руководством, и др.

Для этого можно использовать:

1) компьютерные программы;
2) электронные учебники;
3) тренажеры;
4) диагностические, тестовые и обучающие системы;
5) прикладные и инструментальные программные средства;
6) лабораторные комплексы;
7) системы на базе мультимедиа-технологии;
8) телекоммуникационные системы (например, электронную почту, телеконференции);
9) электронные библиотеки и др.

Весь этот инструментарий должен обеспечивать выполнение конкретных учебных операций:

- обработку текстов;
- составление таблиц и т.д.

Топ-10 облачных провайдеров:

1. *Amazon,* лидер рейтинга.
2. *The Rackspace*.
3. *Google.*
4. *Microsoft.*
5. *Joyent.*
6. *GoGrid.*
7. *Terremark.*
8. *Savvis*.
9. *Verizon.*
10. *NewServer*s.

18.3. Глобальная сеть *Internet*-2

В современном *Internet*, использующем протокол *IPv*4, имеются следующие существенные проблемы, доставшиеся ему «в наследство» от *ARPANET* :

1. *Маленькое адресное пространство* – в современной сети *Internet* используются всего 32-битные адреса (четыре байта на один адрес), т. е. возможно существование около 4 млрд адресов, что меньше не только населения Земли, но и намного меньше количества используемых электронных устройств. Более того, технологически (из-за сегментирования сети на «подсети») невозможно использовать все 4 млрд адресов.

2. *Отсутствие механизма автоматической конфигурации адресов.* Это значительно затрудняет возможность переводить корпоративную сеть от одного провайдера к другому; есть, конечно, внешние сервисы для автоматической конфигурации (*DHCP*), но этот механизм не встроен в протокол – он ставится дополнительным сервисом, т.е. тоже требует дополнительной конфигурации, и т.д.

3. *Низкая производительность из-за фрагментации пакетов*. Дело в том, что слишком большие пакеты *Ethernet* (их максимальный объем составляет 64 кб) могут разбиваться на несколько, поскольку многие сетевые технологии оперируют с блоками меньшего размера. Это действие зачастую производится промежуточными маршрутизаторами, через которые проходит информация. Проблема заключается в том, что разделение пакетов отнимает много системных ресурсов маршрутизатора. Таким образом, этот процесс не только затрудняет перекачку файлов конкретного пользователя, но и потребляет дополнительные ресурсы промежуточных маршрутизаторов.

4. *Неприспособленность к передаче информации, чувствительной к задержкам*. Голосовой трафик, переданный через *Internet*, приходит со случайными задержками, через случайные интервалы, с потерями, что вызывает искажения голоса и характерные для *VoIP* «кваканья». Сегодня же в *Internet* появилось немало новых, в том числе и потоковых, приложений (например, *Streaming Audio* и *Streaming Video*). Для их нормальной работы требуется точное указание и постоянное соблюдение некоторых параметров, таких как пропускная способность, задержка и вариация задержки. Попытки внедрить *QoS* (сервисы обеспечения качества обслуживания) в современный *Internet* особого успеха не принесли, поскольку механизмы *QoS* эффективны внутри высокоскоростных корпоративных сетей, в *Internet* реализовать подобное намного сложнее.

5. *Проблемы безопасности*. Организации, предоставляющие услуги в *Internet*, не могут быть уверены, что на той стороне провода именно тот человек, за кого он себя выдает. Не предприняв специальных мер, пользователи не могут быть уверены, что их финансовая информация не будет украдена или модифицирована при передаче через сеть *Internet*. Обычно нет уверенности, что информация, передаваемая через *Internet*, исходит именно с того адреса, который заявлен в *IP*-пакете как «обратный». Правда, широко используемые сейчас возможности протокола *SSL* практически решают эту проблему.

6. *Невозможность широковещательной передачи данных через Internet*. Превращение *Internet* в универсальную среду передачи информации и, в частности среду для телевещания и радиовещания, тормозится необходимостью передавать каждому зрителю или слушателю свою копию потока данных телепрограммы (хотя многие зрители смотрят одну и ту же телепередачу одновременно).

Все это привело к тому, что в середине 90-х гг. прошлого столетия ряд университетов США совместно с несколькими ведущими корпорациями приступили к работам над созданием новой сети, получившей название *Internet*-2.

Вот так выглядит его логотип:

В настоящее время в проекте принимают участие около 190 университетов. Корпоративными партнерами *Internet*-2 являются такие известные корпорации, как *Microsoft, IBM, Intel,* 3*Com, Cisco, AT&T*.

Internet-2 – это развитие уже привычного *Internet*. Сеть создавалась не на новом месте, при разработке использовались многие наработки, уже прошедшие обкатку на первом варианте сети, поэтому уже через одиннадцать месяцев после начала работ новая сеть была создана. Это был 1997 г.

Первым и основным отличием новой сети от прежней была ее пропускная способность – на самых узких участках сети она не была ниже 100 Мб/с.

Второе отличие в том, что сеть с 2000 г. позиционировалась на использование новой версии протокола *IP* – «*v*.6». Эта версия помимо более высоких скоростей обеспечивает гарантированное качество услуг и решает ряд следующих проблем:

- *IPv* 6 предлагает 128-битные адреса (16 байт, в 4 раза больше, чем было), которые настраиваются абсолютно автоматически, прозрачно для корпоративного пользователя, что позволяет экономить время системных администраторов. В 128-битном адресном пространстве можно разместить столько устройств, сколько потребуется. Общее количество адресов в 128-битном адресном пространстве приблизительно равно $3{,}8 \cdot 10^{38}$, это огромная цифра (в *IPv* 4 было $4{,}3 \cdot 10^{9}$).
- *IPv* 6 предлагает многочисленные улучшения в формате пакета, благодаря чему маршрутизация *IP*-пакета может происходить быстрее и с меньшими затратами вычислительных ресурсов маршрутизаторов. В привычном варианте при потере части пакетов компьютер, который принимает передачу, должен был дожидаться повторной передачи утраченного фрагмента, в результате получаемое видео показывалось с задержками и торможением. Вариант, предложенный для использования в новой сети, требует повторной пересылки только пропавших пакетов, что уменьшает объем передаваемой вторично информации.
- *IPv* 6 гарантирует «качество сервиса», то есть постоянное соблюдение параметров пропускной способности сети и времени переноски пакетов. Видео и *IP*-телефония, передаваемые через континенты через сеть *IPv* 6, имеют гораздо более высокое качество и не страдают от задержек в передаче данных. В новой технологии разделены видео- и аудиопотоки. При получении сигнала система отмечает временным штампом каждый из прибывающих пакетов для дальнейшей синхронизации картинки и звука при показе. Потоковое медиа может поступать на локальную машину со скоростью до 70 Мб/с, что позволяет обеспечивать 12-канальный звук и кристально четкое изображение на экране размерами 90 × 60 см.
- *IPv* 6 поддерживает широковещательную передачу данных (*multicast*, мультикастинг) через сеть. Мультикастинг позволяет передавать лишь одну копию данных (аудио, видео или какой-то другой поток) по общему для нескольких клиентов каналу связи. Тем самым достигается существенная экономия пропускной способности сети и как результат дается «зеленый свет» технологиям видео- и аудиотрансляций через сеть *Internet* в массовом порядке.

В сетевую основу *Internet*-2 заложены высокопроизводительные магистрали передачи данных. Первая из них – *vBNS* (*very high speed Backbone Network Service*) – создана по контракту с корпорацией *MCI WorldCom*. Оптические каналы, используемые для этой сети, обеспечивают пропускную способность 622 Мб/с. Второй магистралью проекта стала сеть под названием *Abilene* (рис. 18.4), созданная на основе национальной оптической сети *Qwest* с использованием технологий *Cisco Systems* и *Nortel* (*Northern Telecom*). Первоначальная пропускная способность этой магистрали составляла 2,5 Гб/с, позднее она была доведена до 100 Гб/с.

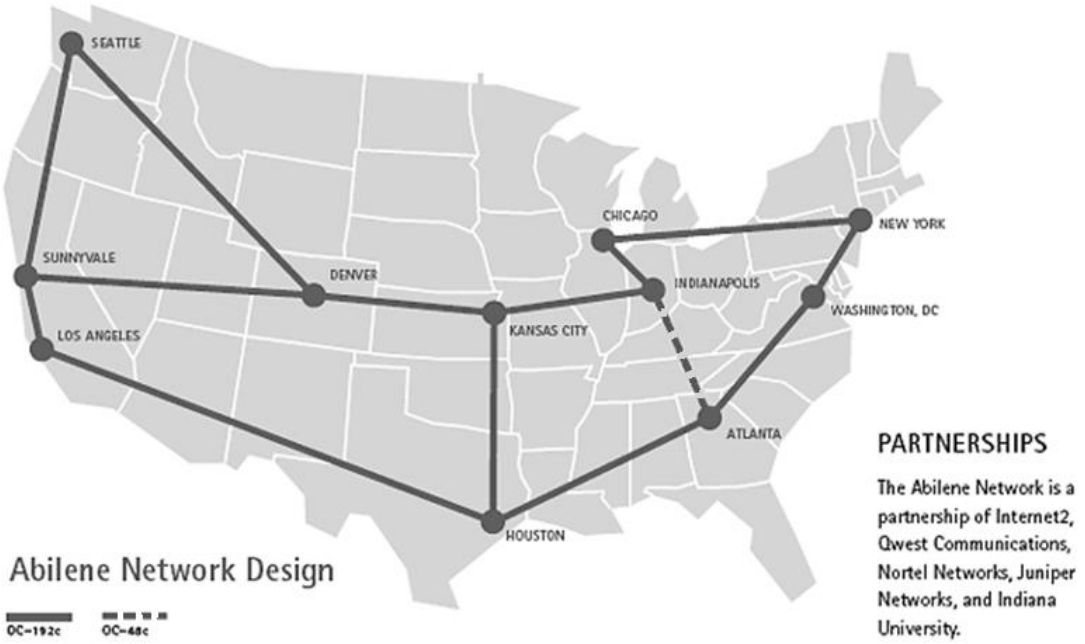


Рис. 18.4. Архитектура сети «*Abilene*»

Для обеспечения такой пропускной способности необходимо и соответствующее оборудование. Этими проблемами занимаются такие известные компании, как *Cisco, Novell* и др.

Развитие магистралей на этом не заканчивается. Консорциум *Internet*-2 принял участие в не менее амбициозном проекте – строительстве *National LambdaRail*, первой трансконтинентальной *Ethernet*-сети. *National LambdaRail* – это оптическая сеть, построенная по технологии *DWDM* (*Dense Wavelength Division MultIPlexing*). По одному волокну

одновременно можно передавать от 32 до 40 каналов, каждому из которых соответствует определенная длина волны (отсюда в названии появилась *Lambda*). Пропускная способность каждого канала – 10 Гб/с.

Оптоволокно пока единственное из средств связи обеспечивает необходимые скорости. В отличие от всех предыдущих вариантов *Ethernet*-сетей 10-гигабитовая технология полностью основана на оптической среде передачи данных (до недавнего времени решения, основанного на медном кабеле, не было). Для каналов доступа и протяженных сетей наилучшим выбором считается одномодовое волокно. Для относительно коротких каналов связи решения могут быть различными. Если говорить об оптоволокне, то его возможности характеризуются следующими цифрами:

- стандартное 50-микронное многомодовое оптоволокно способно передавать данные со скоростью 10 Гб/с на расстояние до 82 м;
- 50-микронное волокно – на расстояние до 66 м;
- 62,5-микронное волокно способно передавать данные с десятигигабитовой скоростью на расстояние до 26 м;
- покрыть расстояние до 300 м позволяет новое 50-микронное многомодовое волокно, оптимизированное для работы с 850-нанометровым лазером (850-*nm laser-optimized*).

Эти решения на данный момент все же являются весьма дорогими. Дешевле использовать медные кабели, но до последнего времени решений, которые могли бы поддерживать столь высокие скорости передачи данных, не было. Лишь в 2006 г. компания *Krone Group* создала первую в мире СКС расширенной категории 6 (*augmented Category* 6), характеристики которой позволяют передавать 10-гигабитовые потоки данных *Ethernet* на расстояние до 100 м. Это решение получило название *CopperTen*.

Продукты *CopperTen* спроектированы таким образом, чтобы межкабельные наводки стали меньше (рис. 18.5). Входящий в состав этой системы кабель имеет уникальную крученую конструкцию (с овальным поперечным сечением), которая создает воздушные зазоры между соседними кабелями, что существенно снижает взаимные наводки.

Рис. 18.5. Канал сети *Internet*-2 на медном кабеле

К сети клиенты подключаются через «точки присутствия» – *gigapops*, они позволяют эффективно использовать пропускную способность всей сети.

По большей части сеть используется для научных целей – дистанционное управление экспериментами, доступ в обсерватории, распределенная обработка огромных массивов данных и, конечно, цифровое видео. Возможность мультикастинга открывает практически безграничные перспективы (в пределах разумного, т.е. общей пропускной способности сети, конечно), поэтому для видеоконференций, а также обычного вещания видео сеть используется весьма активно. Скажем, для дистанционного обучения студентов – трансляция лекций в реальном времени или из архива по сети.

В России первым объявила о вводе в эксплуатацию фрагмента сети, работающего на протоколе *IPv* 6 и обладающего магистралью 10 Гб/с, компания Корбина Телеком. Пока этот сегмент сети охватывает лишь два магистральных узла компании и сеть клиента Корбины – компанию Ниско. Протяженность этого участка сети составляет 28 км.

Если говорить о совместимости сетей *Internet* и *Internet*-2, то имеем обратную совместимость, т.е. из *IPv* 6 пространства можно увидеть *IPv* 4 сеть (старый *Internet*), но не наоборот. Другими словами, клиенты, подключенные к обычному *Internet*, *Internet*-2 сеть увидеть не могут. Но тут уместно внести уточнение – увидеть могут, но не все, а лишь те, кто в состоянии настроить себе туннелирование в *IPv* 6 пространство, используя один из шлюзов *IPv* 4 – *IPv* 6, например *HurriCANe Electric's IPv* 6 *Tunnel Broker*. Компания *HurriCANe Electric* предоставляет свободный доступ в пространство *IPv* 6 через свой

шлюз; достаточно лишь зарегистрироваться, включить у себя поддержку *IPv* 6 стека и соответствующим образом настроить туннелирование трафика.

Вопросы к компьютерному тестированию

1. Назовите протокол, лежащий в основе работы сети *Internet*.
2. Какая из сетей национального масштаба является предшественником *Internet*?
3. Как называют службу поиска и просмотра гипертекстовых документов в *Internet*?
4. Как называют службу телеконференций и группы новостей в *Internet*?
5. Как называют службу передачи электронных сообщений по протоколам *SMTP* и *POP*3 в *Internet*?
6. Какая из служб *Internet* управляет передачей файлов?
7. Какая из служб *Internet* обеспечивает доступ к информации с помощью иерархических каталогов?
8. Как называют службу удаленного доступа к компьютерам в *Internet*?
9. Какова роль модератора в службе телеконференций *Internet*?
10. В чем основное отличие *Web*-страницы от обычных текстовых документов?
11. Как называют команды, с помощью которых браузер выполняет отображение документа на экране?
12. Из чего состоит адрес унифицированного указателя ресурса – *URL* любого файла во всемирной сети?
13. Куда после обработки сервером службы имен доменов направляется запрос на получение одной из страниц сетевого компьютера?
14. Что необходимо ввести при запросе на ввод имени пользователя и связанного с ним пароля *FTP*-сервером с анонимным доступом?
15. Какая из перечисленных служб *Internet* по динамическому *IP*-адресу определяет текущий *IP*-адрес, сообщает его центральной службе и оповещает клиентов?
16. Как называют сетевую технологию, заключающуюся в предоставлении пользователям хостинга удаленного доступа к услугам, вычислительным ресурсам и приложениям через *Internet*?

17. Как называют услугу *Internet* по размещению оборудования клиента на территории провайдера?
18. При какой модели обслуживания предоставляемых услуг облачных технологий потребителю предоставляется только использование программного обеспечения облачного сервиса?
19. При какой модели обслуживания предоставляемых услуг облачных технологий потребителю предлагаются все инфраструктуры сетевого и программного оборудования для управления всеми ресурсами обеспечения облачного сервиса?
20. Какая из известных моделей развертывания облака используется при обслуживании одной организации?
21. Какая из известных моделей развертывания облака является сочетанием двух или более облачных структур, связанных между собой технологиями передачи данных и приложений?
22. Что является причиной ограничения адресного пространства в современной сети *Internet*?
23. Что является причиной ограничения возможности переводить корпоративную сеть от одного провайдера к другому в современной сети *Internet*?
24. Что является причиной низкой производительности в современной сети *Internet*?
25. Что является причиной довольно частого искажения голоса в современной сети *Internet*?
26. Что является первым и основным отличием сети *Internet*-2 от современной сети *Internet*?
27. Какова разрядность адресов протокола *IPv* 6?
28. Что происходит при маршрутизации *IP*-пакетов при передаче видео по технологии *Internet*-2 в случае потери части пакетов?
29. Есть ли разделение аудио- и видеопотоков в *Internet*-2?
30. Как называют прием *Internet*-2, позволяющий передавать лишь одну копию данных (аудио-, видео- или какой-то другой поток) по общему для нескольких клиентов каналу связи?

ЗАКЛЮЧЕНИЕ

Компьютерные сети – это целый мир интереснейших событий, сведений и технологий. Над основными технологиями сетей работают уже несколько десятилетий. Эволюционируют сетевые функции операционных систем, улучшается оборудование, создаётся новое программное обеспечение и всё время появляются новые способы использования вычислительных сетей. Сегодня вычислительные сети продолжают быстро развиваться. Разрыв между локальными и глобальными сетями постоянно сокращается во многом из-за появления высокоскоростных территориальных каналов связи, не уступающих по качеству кабельным системам локальных сетей.

В глобальных сетях появляются службы доступа к ресурсам, такие же удобные и прозрачные, как и службы локальных сетей. Подобные примеры в большом количестве демонстрирует самая популярная глобальная сеть *Internet*.

Изменяются и локальные сети. Появилось разнообразное коммуникационное оборудование – коммутаторы, маршрутизаторы, шлюзы. Благодаря такому оборудованию имеется возможность построения больших корпоративных сетей, имеющих сложную структуру. Быстро и успешно развиваются беспроводные сети, сейчас уже можно говорить, что они конкурируют с традиционными сетями, построенными на кабельных линиях связи.

Проявилась еще одна очень важная тенденция, затрагивающая в равной степени как локальные, так и глобальные сети. Стали применяться методы обработки аудио- и видеоинформации в сетях. Сложность передачи такой информации, получившей название мультимедийной, по сети связана с ее чувствительностью к задержкам при передаче: задержки обычно приводят к искажению информации в конечных узлах сети.

Сегодня эти проблемы решаются различными способами, но, несмотря на значительные усилия, предпринимаемые в этом направлении, до приемлемого решения проблемы пока далеко. Компьютерные сети уже сегодня работают на пределе своих возможностей, и нагрузку, которую предстоит испытать сетям при таком активном росте, они

могут просто не выдержать. Развитие всех перечисленных тенденций возможно только после внедрения новой, более гибкой архитектуры компьютерных сетей.

Самая перспективная на сегодня технология/архитектура компьютерных сетей, которая способна вывести из кризиса, – это технология программно-конфигурируемых сетей (ПКС). Ее основная ценность в том, что она позволяет уйти от «ручного» управления сетью, выводя на первый план программное обеспечение. В современных сетях функции управления и передачи данных совмещены, что делает контроль и управление очень сложными. ПКС-архитектура разделяет процесс управления и процесс передачи данных, что открывает колоссальные возможности для развития интернет-технологий.

К основным направлениям и путям развития компьютерных сетей можно отнести следующие:

1. Развитие топологии сетей, направленное на обеспечение одновременного обслуживания запросов от большего количества абонентских систем и увеличение оперативности и надежности доставки пакетов адресатам за счет создания альтернативных маршрутов.

2. Создание новых, более совершенных протоколов обмена информацией и управления сетями, развитие информационных и телекоммуникационных технологий.

3. Совершенствование существующих и создание новых аппаратных средств передачи и обработки информации

4. Развитие программного обеспечения сетей.

5. Повышение надежности сетей по всем аспектам – техническому, программному, информационному, функциональному.

6. Развитие методов и средств обеспечения более высокого уровня безопасности информации, циркулирующей в сетях.

7. Расширение перечня предоставляемых информационно-вычислительных услуг.

8. Рациональная организация обслуживания очередей запросов пользователей сети.

9. Повышение эргономичности компьютерных сетей, достигаемое путем оптимизации трудовой деятельности пользователей сети, ее управленческого и обслуживающего персонала.

10. Создание и непрерывное совершенствование глобальной интеллектуальной сети, объединяющей сети всех государств. В рамках такой сети вполне реально решение задачи по удовлетворению запроса пользователя из любой точки планеты и в любое время.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Колдаев, В. Д. Архитектура ЭВМ : учеб. пособие / В. Д. Колдаев, С. А. Лупин. – М. : Форум : НИЦ ИНФРА-М, 2014. – 384 с. – ISBN 978-5-8199-0373-5.

2. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации : учеб. пособие для вузов / В. Л. Бройдо, О. П. Ильина. – 4-е изд., стер. – СПб. : Питер, 2011. – 554 с. – (Учебник для вузов). – ISBN 978-5-49807-875-5.

3. Введение в инфокоммуникационные технологии : учеб. пособие / Л. Г. Гагарина [и др.] ; под ред. проф. Л. Г. Гагариной. – М. : Форум : НИЦ ИНФРА-М, 2013. – 336 с. – ISBN 978-5-8199-0551-7.

4. Горнец, Н. Н. Организация ЭВМ и систем: учеб. пособие для вузов по направлению 230100 «Информатика и вычислительная техника» / Н. Н. Горнец, А. Г. Рощин, В. В. Соломенцев. – М. : Академия, 2006. – 316 с. – ISBN 5-7695-2269-0.

5. Горнец, Н. Н. ЭВМ и периферийные устройства. Компьютеры и вычислительные системы : учеб. для вузов по направлению «Информатика и вычислительная техника» / Н. Н. Горнец, А. Г. Рощин. – М. : Академия, 2012. – 234 с. – ISBN 978-5-7695-8720-7.

6. Дроздова, Е. Н. Компьютерные сети. Компоненты, протоколы, технологии / Е. Н. Дроздов. – СПб. : Петербургский ин-т печати, 2006. – 160 с. – ISBN 5-934220-28-4.

7. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд., стер. – СПб. : Питер, 2010. – 944 с. – ISBN 978-5-49807-389-7.

8. Кузин, А. В. Компьютерные сети : учеб. пособие / А. В. Кузин. – 3-е изд., перераб. и доп. – М. : Форум : НИЦ ИНФРА-М, 2014. – 192 с. – ISBN 978-5-91134-476-4.

9. Максимов, Н. В. Компьютерные сети : учеб. пособие для студенческих учреждений СПО / Н. В. Максимов, И. И. Попов. – 6-е изд., перераб. и доп. – М. : Форум : НИЦ ИНФРА-М, 2013. – 464 с. – ISBN 978-5-91134-764-2.

10. Кравец, О. Я. Практикум по вычислительным сетям и телекоммуникациям / О. Я. Кравец. – Воронеж : Научная книга, 2007. – 156 с. – ISBN 978-5-98222-200-8.

11. Мелехин, В. Ф. Вычислительные машины, системы и сети : учеб. для вузов по направлению «Автоматизация и управление» / В. Ф. Мелехин, Е. Г. Павловский. – 2-е изд., стер. – М. : Академия, 2007. – 555 с. – ISBN 978-5-7695-4485-9.

12. Телекоммуникации. Руководство для начинающих / М. Мур [и др.]. – СПб. : БХВ-Петербург, 2005. – 624 с. – ISBN 5-94157-249-2.

13. Новожилов, О. П. Архитектура ЭВМ и систем : учеб. пособие для бакалавров. – М. : Юрайт, 2015. – 527 с. – ISBN 978-5-9916-2695-8.

14. Виснадул, Б. Д. Основы компьютерных сетей : учеб. пособие / Б. Д. Виснадул, С. А. Лупин, С. В. Сидоров ; под ред. Л. Г. Гагариной. – М. : Форум : НИЦ ИНФРА-М, 2012. – 272 с. – ISBN 978-5-8199-0294-3.

15. Основы построения систем и сетей передачи информации / В. В. Ломовицкий [и др.] ; ред. В. М. Щекотихин. – М. : Горячая линия-Телеком, 2005. – 382 с. – ISBN 5-93517-201-1.

16. Основы построения телекоммуникационных систем и сетей / ред. В. Н. Гордиенко, В. И. Крухмалев. – М. : Горячая линия-Телеком, 2004. – 510 с. – ISBN 5-93517-202-X.

17. Палмер, М. Проектирование и внедрение компьютерных сетей / М. Палмер, Р. Б. Синклер. – СПб. : БХВ-Петербург, 2004. – 752 с. – ISBN 5-94157-374-X.

18. Пескова, С. А. Сети и телекоммуникации / С. А. Пескова, А. В. Кузин, А. Н. Волков. – М. : Академия, 2006. – 352 с. – ISBN 978-5-7695-4149-0.

19. Попов, В. Б. Основы информационных и телекоммуникационных технологий: Сетевые информационные технологии / В. Б. Попов. – М. : Финансы и статистика, 2005. – 224 с. – ISBN 5-279-03013-9.

20. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации : учеб. для вузов по специальности «Прикладная информатика в экономике» / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко ; под ред. А. П. Пятибратова. – изд. 2-е, перераб. и доп. – М. : Финансы и статистика, 2014. – 509 с. – ISBN 5-279-02301-9.

21. Семенов, Ю. А. Алгоритмы телекоммуникационных сетей : в 3 ч. / Ю. А. Семенов. – М. : *Internet*-Ун-т Информ. технологий : БИНОМ. Лаборатория знаний, 2007. – (Основы информ. технологий). – Ч. 1 : Алгоритмы и протоколы каналов и сетей передачи данных. – 637 с. – ISBN 978-5-94774-706-5 ; Ч. 2 : Протоколы и алгоритмы маршрутизации в INTERNET. – 828 с. – ISBN 978-5-94774-707-2.

22. Степанов, А. Н. Архитектура вычислительных систем и компьютерных сетей / А. Н. Степанов. – СПб. : Питер, 2007. – 509 с. – ISBN 978-5-469-01451-5.

23. Хандадашева, Л. Н. Программное обеспечение. Вычислительные сети / Л. Н. Хандадашева, И. Г. Истомина. – М. : ИКЦ «МарТ» ; Ростов н/Д. : МарТ, 2005. – 320 с. – ISBN 5-241-00486-6.

24. Шарипов, Ю. К. Отечественные телекоммуникационные системы / Ю. К. Шарипов, В. К. Кобляков. – М. : Логос, 2005. – 832 с. – ISBN 5-94010-288-3.

Периодические издания

1. Периодическое издание «Журнал сетевых решений/*LAN*» – *Online* версия. Русский ресурс.

2. Периодическое издание «Сети» – *Online* версия. Русский ресурс.

3. Периодическое издание «Сетевой журнал» – *Online* версия. Русский ресурс.

4. Периодическое издание «Сети и системы связи» – *Online* версия. Русский ресурс.

Internet-ресурсы

1. Брежнев, А. Ф., Смелянский Р. Л. Семейство протоколов *TCP/IP* / А. Ф. Брежнев, Р. Л. Смелянский. – URL: http://www.mark-itt.ru/FWO/tcpIP (дата обращения: 25.12.2016).

2. Электронные лекции «Современные сетевые технологии», РТУиС, МИЭМ, г. Москва. – URL: http://network.distudy.ru/index.html (дата обращения: 25.12.2016).

3. Якушин, А. В. Компьютерные сети. *Internet* и мультимедиа технологии. Лекционный курс / А. В. Якушин. – URL: http://www.tula.net/tgpu/resources/yakushin/html_doc/doc02/doc02index.htm (дата обращения: 25.12.2016).

4. Новейшие компьютерные технологии. – URL: http//www.citforum.ru/ (дата обращения: 25.12.2016).

5. Последние новости в компьютерном мире. – URL: http//www.iXBT.ru (дата обращения: 25.12.2016).

6. Достижения суперкомпьютерной техники. – URL: http//www.supercomputers.ru (дата обращения: 25.12.2016).

7. Сайт-справочник по сетевым технологиям, протоколам, интерфейсам. Русские ресурсы. – URL: http://www.protocols.ru/WP/ (дата обращения: 25.12.2016).

8. Ресурс информации и полезных ссылок на техническую информацию о современных информационных технологиях, в том числе и сетевых. – URL: http://www.techfest.com/ (дата обращения: 25.12.2016).

ГЛОССАРИЙ

Абоненты сети

Объекты, генерирующие или потребляющие информацию в сети (это могут быть: отдельные ЭВМ, комплексы ЭВМ, терминалы, промышленные роботы, станки с числовым программным управлением и т.д.). Любой абонент сети подключается к станции.

Аппаратное обеспечение (*Hardware*)

Физическое оборудование, составляющее вашу сеть.

Архитектура (*Architecture*)

Способ организации сети, при помощи которого информация передается между компьютерами, входящими в сеть.

Архитектура *Ethernet* (*Ethernet architecture*)

Наиболее популярная и наименее затратная сетевая архитектура, включающая в себя следующие топологии: «звезда», последовательное соединение, «кольцо» и гибридные виды.

Архитектура *TokenRing* (*TokenRing architecture*)

Архитектура, зачастую используемая в крупных организациях, но в настоящий момент практически устаревшая.

База данных поисковой системы

Набор всей информации, к которой вы можете получить доступ. База данных скрыта от пользователя, но именно в ней компьютер ведет поиск, когда вы направляете свой поисковый запрос.

Брандмауэр (*Firewall*)

Программное и/или аппаратное обеспечение, предназначенное для защиты компьютера или сети от угроз извне.

Веб-браузер, браузер (*Web browser*)

Программное обеспечение, которое отображает веб-страницы, включая текст, графику и другое мультимедиа содержимое, например музыку.

Веб-сайт (*Web site*)

Группировка похожей информации во Всемирной паутине, состоящая из индивидуальных веб-страниц.

Веб-сайт с древовидной структурой (*Tree web site*)

Сайт, который организован подобно генеалогическому древу с набором различных опций и настроек для просмотра информации на сайте.

Веб-страница (*Web page*)

Индивидуальная страница, содержащая определенную информацию. Набор сгруппированных веб-страниц образует веб-сайт.

Витая пара (*Twisted pair cable*)

Кабель, состоящий из одной или более пар перевитых между собой медных проводов.

Всемирная паутина (*World Wide Web, WWW*)

Набор страниц и сайтов в Интернете, созданных для просмотра веб-браузером. Также известна под названием «Паутина», или веб.

Вычислительная сеть

Совокупность ЭВМ, объединённых средствами передачи данных.

Гибридная сеть (*Hybrid mesh network*)

Сеть, которая сочетает в себе как минимум две разные топологии построения.

Гигабитный Ethernet (*Gigabit Ethernet*)

Новая, более быстрая архитектура Ethernet, которая передает информацию более чем в десять раз быстрее по сравнению с архитектурой *Fast Ethernet*.

Гиперссылка (*Hyperlink*)

Ссылка на веб-сайте, которая позволяет вам перемещаться между веб-страницами. Гиперссылка обычно отображается подчеркнутым текстом, часто синего цвета.

Глобальная сеть

Вычислительная сеть объединяет абонентов, расположенных в различных странах, на различных континентах. Абоненты такой сети могут взаимодействовать на базе телефонных линий связи, радиосвязи и систем спутниковой связи.

Динамический *IP*-адрес (*Dynamic IP address*)

IP-адрес, который назначается каждый раз, когда компьютер входит в сеть на время онлайн сессии.

Дискуссионная группа, список рассылки (*Discussion list*)

Группа людей, общающихся при помощи электронной почты, имеющих общие интересы и общий адрес, почта на который идет всем находящимся в списке.

Домен верхнего уровня (*Top-level domain, TLD*)

Суффикс в доменном имени, который демонстрирует тип сервера, хранящего веб-сайт, например: *.com* (коммерческий) или *.edu* (образовательный).

Доменное имя (*Domain name*)

Имя сервера, который содержит всю информацию веб-сайта, например *microsoft.com*.

Защищенная (экранированная) витая пара (*Shielded Twisted Pair, STP*)

Одна или несколько пар медных проводов, которые покрыты защитным металлом или фольгой под пластиковым кожухом, обеспечивающими защиту от помех и сохраняющими целостность данных.

Звезда-кольцо

Периферийные концентраторы в звезде-кольце подсоединены к главному концентратору.

Звезда-шина

Несколько сетей с топологией «звезда» объединяются при помощи магистральной линейной шины (к концентратору подключены компьютеры, а сами концентраторы соединены шиной).

Интернет (*Internet*)

Самая известная и большая в мире компьютерная сеть, соединяющая миллионы компьютеров в одну огромную сеть сетей.

Интерфейс (*Interface*)

Окно, которое вы видите на веб-сайте.

Кабель-канал (*Conduits*)

Полая трубка, используемая для защиты кабеля от механических повреждений.

Канальный уровень

Реализует процесс передачи данных по информационному каналу.

Клиент (*Client*)

Компьютер в сети, подсоединяющийся к серверу для получения информации.

Коаксиальный кабель (*Coaxial cable*)

Кабель, выполненный в соответствии с уже устаревшим промышленным стандартом. Похож на кабель для подключения телевизионных антенн. Состоит из медного сердечника в изолирующем слое пластмассы. Поверх этого слоя – экранирующее покрытие металлической оплетки или фольги и защитный слой.

Кольцевая сеть, закольцованная сеть (*Ring network*)

Сеть, построенная на основе непрерывного кабеля, соединяющего компьютеры, которые объединены им в кольцо.

Коммуникационный сервер (*Communications server*)

Устройство или компьютер, который предоставляет пользователям локальной сети прозрачный доступ к своим последовательным портам ввода/вывода.

Коммутатор (*Switch*)

Центральное соединительное устройство, похожее на концентратор. Получая информацию из сети, коммутатор отправляет ее в конкретное место назначения в этой сети.

Компьютерная (вычислительная) сеть

Совокупность компьютеров и терминалов, соединенных с помощью каналов связи в единую систему, удовлетворяющую требованиям распределенной обработки данных.

Куки (*Cookie*)

Небольшой текстовый файл, содержащий информацию о вашем предыдущем визите на веб-сайт.

Локальная сеть

Вычислительная сеть объединяет абонентов, расположенных в пределах небольшой территории.

Магистральная сеть

Объединяет отдельные сети доступа, выполняя функции транзита трафика между ними по высокоскоростным каналам.

Маршрутизатор (*Router*)

Сетевое оборудование, которое соединяет разные сети и направляет, или маршрутизирует, информацию между компьютерами в сети.

Модем (*Modem*)

Сетевое оборудование, которое подключает компьютер к Интернету посредством телефонной линии.

Незащищенная витая пара (*Unshielded Twisted Pair, UTP*)

Самый дешевый кабель в настоящее время, сделан из одной или более пар медных проводов без какой-либо защиты.

Одноранговая сеть (*Peer-to-Peer Network*)

Сеть, которая объединяет равноправные компьютеры.

Окончание, терминатор (*Terminator*)

Устройство, размещаемое на каждом конце кабеля в сети последовательного подключения устройств.

Оптоволоконный кабель (*Fiber optic cable*)

Кабель, который в отличие от обычного кабеля вместо электрических импульсов передает импульсы света. Самый дорогостоящий вид кабеля, рассчитанный на большие расстояния.

Повторитель (*Repeater*)

Устройство, усиливающее или регенерирующее пришедший на него сигнал.

Подмена *DNS* (*DNS spoofing*)

Изменение *DNS*-записи таким образом, что она ведет на другой веб-сайт.

Подмена внешнего вида веб-страницы (*Web page defacement*)

Нелегальный доступ к веб-сайту с целью изменения его внешнего вида и информации.

Поисковая система (*Search Engine*)

Веб-сайт, на котором вы можете найти интересующую вас информацию, используя набор ключевых слов.

Поисковая система по метаданным (*Meta Search Engine*)

Веб-сайт с системой, которая исследует огромное количество сайтов поисковых систем и комбинирует для вас полученные результаты.

Порт (*Port*)

Розетка на соединительном устройстве, в которую подключается кабель от компьютерного оборудования. Центральное соединительное устройство обычно содержит несколько портов.

Представительный уровень

Определяет синтаксис данных в модели *OSI*, т.е. представление данных в кодах и форматах, принятых в данной системе. Осуществляет трансформацию различных языков, форматов данных и кодов для взаимодействия разнотипных компьютеров.

Прикладной уровень

Содержит все необходимые элементы сервиса, обеспечивает поддержку прикладных программ конечных пользователей, т.е. управляет общим доступом к сети.

Провайдер услуг Интернет (*Internet Service Provider, ISP*)

Компания, предоставляющая доступ в Интернет. Оплата услуг может осуществляться повременно или на основе учета трафика.

Программное обеспечение против спама (*Anti-spam software*)

Программное обеспечение, которое фильтрует спам.

Пропускная способность (*Bandwidth*)

Количество информации, которое может быть передано через сетевое соединение за одну единицу времени.

Протокол (*Protocol*)

Набор правил, которые помогают компьютерам «понимать» друг друга.

Протокол безопасного соединения (*Secure Sockets Layer, SSL*)

Набор правил, или протокол, используемый для безопасной передачи информации.

Протокол передачи гипертекста (*Hypertext Transfer Protocol, HTTP*)

Набор правил, или протокол, используемый для отправки и получения информации по Всемирной паутине.

Протокол передачи файлов (*File Transfer Protocol, FTP*)

Набор правил, или протокол, который управляет перемещением или копированием файлов с одного компьютера на другой.

Протокол управления передачей данных/межсетевой Интернет-протокол (*Transmission Control*)

Протокол, который управляет межсетевым перемещением или копированием файлов.

Рабочая станция (*Workstation*)

Персональный компьютер, подключенный к сети, на котором пользователь сети выполняет свою работу.

Распределенная обработка данных

Обработка данных, выполняемая на независимых, но связанных между собой компьютерах, представляющих распределенную систему.

***Protocol/Internet Protocol* (*TCP/IP*)**

Набор правил, или протокол, который обеспечивает отправку и получение информации по сети Интернет.

Региональная сеть

Вычислительная сеть связывает абонентов, расположенных на значительном расстоянии друг от друга. Она может включать абонентов внутри большого города, экономического региона, отдельной страны. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки-сотни километров.

Режим реального времени (*Real Time*)

Режим, при котором не существует ощутимых промежутков времени между отправкой информации по Интернету одним человеком и ее получением другим через открытое соединение между ними.

Рекламное програмное обеспечение (*Adware*)

Программное обеспечение, демонстрирующее рекламу, всплывающую на вашем экране, когда программа работает.

Сеансовый уровень

Реализует установление и поддержание сеанса связи между абонентами через коммуникационную сеть. Он управляет диалогом между взаимодействующими процессами.

Сервер (*Server*)

Компьютер в сети клиент-сервер, который хранит всю информацию и ресурсы, а также обеспечивает доступ к ним с других компьютеров в сети.

Сервер баз данных

Компьютер, выполняющий функции хранения, обработки и управления файлами баз данных (БД).

Сервер доменных имен (*Domain Name Server, DNS*)

Сервер, который преобразует IP-адрес в доменное имя и наоборот.

Сервер доступа (*Access server*)

Выделенный компьютер, позволяющий выполнять удаленную обработку заданий. Программы, инициируемые с удаленной рабочей станции, выполняются на этом сервере.

Сервер печати (*Print server*)

Сервер, который управляет процессом печати и хранит все задания для принтера, посланные со всех компьютеров в сети.

Сетевая операционная система (*Network Operating System, NOS*)

Программное обеспечение, которое контролирует, организует и управляет всей деятельностью, происходящей в сети.

Сетевой уровень

Отвечает за выбор маршрута передачи пакетов по линиям, связывающим узлы коммуникационной сети, т.е. реализует межсетевое взаимодействие.

Сервер прикладных программ (*Application server*)

Компьютер, который используется для выполнения прикладных программ пользователей.

Сервер резервного копирования данных (*Back up server*)

Устройство или компьютер, который решает задачи создания, хранения и восстановления копий данных, расположенных на файловых серверах и рабочих станциях.

Сетевой этикет (*Netiquette*)

Набор правил для написания электронных почтовых сообщений.

Сервер сети (*Server*)

Компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, например, хранение данных общего пользования, печать заданий, обработку запроса к СУБД, удаленную обработку заданий и т.д.

Сетевая топология

Обобщенная геометрическая характеристика компьютерной сети. Определяет схему физического подключения компьютеров в единую сеть.

Сетевой адаптер (*Network Interface Card, NIC*)

Аппаратное обеспечение, установленное внутри компьютера, которое подсоединяет его к сети.

Сеть (*Network*)

Группа компьютеров, соединенных каким-либо способом так, что люди могут обмениваться информацией и совместно использовать оборудование.

Сеть звездная (*star*)

Центральный узел, от которого расходятся линии передачи данных к каждому из остальных узлов.

Сеть клиент-сервер (*Client/Server Network*)

Сеть, в которой выделенный компьютер содержит всю информацию и ресурсы, предоставляя доступ к ним другим компьютерам, находящимся в сети.

Сеть кольцевая (*ring*)

Узлы связаны кольцевой линией передачи данных (к каждому узлу подходят только две линии); данные, проходя по кольцу, поочередно становятся доступными всем узлам сети.

Сеть с шинной организацией (*Bus network*)

Сеть, в которой все компьютеры подсоединяются вдоль одного кабеля, также называемого опорным (*backbone*).

Сеть с шиной типа «звезда» (*Star bus network*)

Сеть, в которой каждый компьютер присоединяется к центральной точке сети. Одна из самых часто применяемых в настоящее время сетевых топологий.

Сеть шинная (*bus*)

Локальная сеть, в которой связь между любыми двумя станциями устанавливается через один общий путь, и данные, передаваемые любой станцией, одновременно становятся доступными для всех других станций, подключенных к этой же среде передачи данных (последнее свойство называют широковещательностью).

Служба передачи файлов (*FTP*)

Служба *FTP* имеет свои серверы в мировой сети, на которых хранятся архивы данных.

Служба телеконференций (*Usernet*)

Рассылка электронной почты, в ходе которой одно сообщение отправляется не одному корреспонденту, а большой группе (такие группы называются телеконференциями, или группами новостей).

Служба удаленного управления компьютером (*Telnet*)

Подключившись к удаленному компьютеру по протоколу этой службы, можно управлять его работой. Такое управление еще называют консольным, или терминальным.

Совместное использование файлов в одноранговой сети (*Peer-to-Peer file sharing*)

Использование файлов в сети Интернет совместно с другими пользователями непосредственно с вашего компьютера.

Соединение класса *T*1 (*T*1 *connection*)

Соединение, которое используется компаниями и зачастую небольшими провайдерами для подключения к сети Интернет на скорости приблизительно 1,544 Мб/с.

Соединение класса *T*3 (*T*3 *connection*)

Соединение, в котором используется оптоволоконный кабель для передачи информации на скоростях до 44,73 Мб/с.

Списки рассылки (*Mail List*)

Специальные тематические серверы, собирающие информацию по определенным темам и переправляющие её подписчикам в виде сообщений электронной почты.

Среда передачи данных (*Transmission media*)

Другое название кабельной или беспроводной сети, используемой для передачи данных.

Станция

Аппаратура, которая выполняет функции, связанные с передачей и приемом информации.

Статический *IP*-адрес (*Static IP address*)

Фиксированный *IP*-адрес, назначаемый определенному компьютеру. Статический *IP* адрес является необходимым для веб-серверов.

Стек протоколов *TCP/IP* (*TCP/IP Protocol Suite*)

Набор протоколов, или правил, которые управляют передачей информации по сети Интернет.

Сцепление гирляндой (*Daisy chaining*)

Вид соединения нескольких концентраторов.

Топология (*Topology*)

Структура или тип построения и разводки сети, часто зависит от сетевой архитектуры.

Топология ЛВС

Усредненная геометрическая схема соединений узлов сети.

Транспортный уровень

Обеспечивает сопряжение абонентов сети с базовой сетью передачи данных.

Трассировщики пакетов (*Packet sniffers*)

Программы, которые наблюдают за информацией в сети.

Узел

Любое устройство, непосредственно подключенное к передающей среде сети.

Универсальная поисковая система (*General Purpose Search Engine*)

Поисковая система, охватывающая широкий спектр информации, удобна для поиска неспециализированной информации.

Универсальный локатор ресурса (*Uniform resource locator, URL*)

Адрес веб-сайта во Всемирной паутине, например http://www.microsoft.com.

Устройство хранения информации, накопитель (*Storage device*)

Устройство, на котором вы храните файлы, например, жесткий диск, компакт диск, ленточный и оптический приводы.

Факс-сервер (*Fax server*)

Устройство или компьютер, который выполняет рассылку и прием факсимильных сообщений для пользователей локальной сети.

Физическая передающая среда

Линии связи или пространство, в котором распространяются электрические сигналы, и аппаратура передачи данных.

Физический уровень

Выполняет все необходимые процедуры в канале связи, обеспечивая передачу потока битов по физической передающей среде.

Хаб, концентратор (*Hub*)

Центральное соединительное устройство, к которому присоединяются все сетевые кабели.

Цифровая абонентская линия (*Digital Subscriber Line, DSL*)

Вид подключения, который использует существующую телефонную линию для установки постоянного интернет-соединения на высокой скорости от 1 до 9 Мб/с.

Цифровая сеть интегрированного обслуживания (*Integrated Services Digital Network, ISDN*)

Вид подключения, который передает информацию со скоростью 128 кб/с.

Чат (*Chat*)

Программа, позволяющая группам людей общаться в реальном времени, используя Интернет.

Шифрование (*Encryption*)

Процесс кодирования пересылаемой информации таким образом, чтобы ее мог прочитать только человек или компьютер, которому она предназначена.

Шлюз (*Gateway*)

Устройство сопряжения, которое соединяет два разных типа сетей. Шлюз получает информацию, переводит ее, а затем пересылает перевод по месту назначения.

Электронная почта (*Electronic mail, e-mail*)

Корреспонденция, пересылаемая по Интернету.

Язык гипертекстовой разметки (*Hypertext markup language, HTML*)

Язык программирования, используемый для создания веб-страниц.

Ячеистая топология

Сеть с ячеистой топологией обладает высокой избыточностью и надежностью, так как каждый компьютер в такой сети соединен с каждым другим отдельным кабелем.

***ANSI*-136**

Североамериканский цифровой стандарт мобильной связи, используемый в системах *TDMA* (ранее *D-AMPS*).

***CIFS* (*Common Internet File System*, общая файловая система Интернета)**

Протокол уровня приложений, обеспечивает доступ к файлам и сервисам на удаленных компьютерах на основе клиент-серверной модели взаимодействия в корпоративных сетевых системах хранения данных; традиционно используется в ЛВС с ОС *Windows* для доступа к файлам через транспортный протокол *TCP/IP*.

***DAFS* (*Direct Access File System*, прямой доступ к файловой системе)**

Стандартный протокол файлового доступа, основанный на *NFS*; позволяет прикладным задачам передавать данные в обход операционной системы и ее буферного пространства напрямую к транспортным ресурсам.

***DDI* (*Copper Distributed Data Interface*, распределенный интерфейс передачи данных по медному кабелю)**

Спецификация фирмы *Crescendo Communications* для передачи трафика *FDDI* по медному кабелю (в 1993 г. эта фирма была приобретена ведущим производителем маршрутизаторов – компанией *Cisco Systems*). Спецификация *CDDI* положена в основу стандарта *TP-PMD*.

***EIA/TIA*-232**

Стандарт для 25-контактного последовательного интерфейса, который может быть использован для подсоединения компьютеров к сетевому оборудованию (старое название – *RS*-232).

***FDDI* (*Fiber Distributed Data Interface*)**

Стандарт на распределенный интерфейс высокоскоростной передачи данных по волоконно-оптическому кабелю, принятый комитетом *ANSI X*3*t*9.5 в 1989 г. Стандарт состоит из четырех частей: двух подуровней семиуровневой модели *OSI* – *PMD* и *MAC*, а также протоколов *PHY* и *SMT*.

***IETF* (*Internet Engineering Task Force*, Инженерная проблемная группа Интернета)**

Международная общественная организация сообщества Интернета, которая отвечает за организацию работы системы, разработку стандартов сети и техническое усовершенствование средств ее обеспечения.

***IRC* (*Internet Realy Chat*)**

Служба предназначена для прямого общения нескольких человек в режиме реального времени – чат-конференции, или чаты.

***MRCP* (*Media Resource Control Protocol*, протокол управления медиа-ресурсами)**

Созданый *IETF* универсальный прикладной протокол, который предоставляет голосовым приложениям в сетях *VoIP* доступ к службам медиа-серверов через независимый от производителя программный интерфейс *API*.

***NFS* (*Network File System*, сетевая файловая система)**

Совокупность распределенной файловой системы и сетевого протокола, традиционно применяемая на платформах *UNIX* в клиент-серверных вычислительных сетях. Система использует транспортный протокол *TCP/IP* и обеспечивает доступ к файлам на удаленном сервере. Для работы в *WWW* был разработан *WebNFS*.

***PHY* (*PHYsical layer protocol*)**

Протокол физического уровня стандарта *FDDI*, который определяет часть физического уровня, не зависящую от среды передачи данных: средства их кодирования и декодирования, схему синхронизации и набор сигналов управления. Протокол отделяет канальный уровень от подуровня *PMD*.

RS*232-*C

Стандарт *EIA* на интерфейс для соединения оконечных цифровых устройств ООД (*DTE*) и АПД (*DCE*).

***RS*422**

Стандарт *EIA*, рекомендуемый вместо *RS*232 при длине кабеля более 15 м. Стандарт определяет электрические характеристики

цифровых цепей со сбалансированным напряжением, совместим по электрическим параметрам со стандартом *ITU-T V.*11; использует коннекторы *DB*-25.

***RS*423**

Стандарт *EIA*, рекомендуемый вместо *RS*232 при длине кабеля более 15 м. Стандарт определяет электрические характеристики цифровых цепей с несбалансированным напряжением, совместим по электрическим параметрам со стандартом *ITU-T V.*10; предложен одновременно с *RS*422, однако используется реже.

***SMT* (*Station Management*)**

Протокол управления станцией стандарта *FDDI*, описывающий процессы управления станциями и концентраторами, инициализацией и поддержанием соединений между узлами, а также алгоритмы обнаружения ошибок и обработки аварийных ситуаций. В соответствии с протоколом *SMT* адаптеры *FDDI* автоматически выполняют большинство функций управления.

***SPF* (*Open Shortest Path First*, открытый протокол предпочтения кратчайшего пути)**

Стандарт и протокол, разработанные комитетом *IETF* для маршрутизаторов сети Интернет в целях определения оптимального маршрута передачи данных.

***TP-PMD* (*Twisted Pair Physical Medium Dependent*)**

Стандарт *ANSI* для реализации *FDDI* на основе неэкранированной витой пары пятой категории с коннекторами *RJ*-45 или экранированной витой пары категории *IBM Type* 0,5 с коннекторами *DB*-9. В основу *TP-PMD* положена спецификация *CDDI*.

Учебное издание

ГАЛАС Валерий Петрович

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ, СЕТИ
И ТЕЛЕКОММУНИКАЦИИ

Учебник

Часть 2. Сети и телекоммуникации

Редактор А. А. Амирсейидова
Технический редактор С. Ш. Абдуллаева
Корректор О. В. Балашова
Компьютерная верстка Е. А. Герасиной
Дизайн обложки В. П. Галаса

Подписано в печать 20.12.17.
Формат 60×84/16. Усл. печ. л. 16,51. Тираж 60 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.