

МГАПИ

**МОСКОВСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ
ПРИБОРОСТРОЕНИЯ И ИНФОРМАТИКИ**

Кафедра “Персональные компьютеры и сети”

Брейман А.Д.

Сети ЭВМ и телекоммуникации
Учебное пособие

Часть 1
Общие принципы построения сетей
Локальные сети

Москва, 2001

УДК 681.326(075)

Сети ЭВМ и телекоммуникации. Учебное пособие. Часть 1. Общие принципы построения сетей. Локальные сети. /Брейман А.Д. – М.:МГАПИ, 2001. – 75с.:ил.

Настоящее пособие предназначено для подготовки студентов различных форм обучения по специальностям: 22.01, 22.03.

Пособие предназначено для подготовки студентов, изучающих принципы построения компьютерных сетей и технологии, используемые в локальных вычислительных сетях.

Для специальности 22.01 данное учебное пособие может быть использовано при изучении курсов “Сети и средства телекоммуникаций” и “Администрирование сетевых систем”.

Работа рассмотрена и одобрена на заседании кафедры ИТ-4 “Персональные компьютеры и сети”.

© Брейман А.Д., 2001
© МГАПИ, 2001

АННОТАЦИЯ

Рекомендовано Ученым Советом МГАПИ в качестве учебного пособия для специальности 22.01 “Вычислительные машины, комплексы, системы и сети”.

Настоящее пособие предназначено для подготовки студентов, изучающих принципы построения компьютерных сетей и технологии, используемые в локальных сетях. Рассмотрены принципы построения компьютерных сетей и телекоммуникационных систем, модели взаимосвязи систем, применяемые для описания сетей, основы передачи данных, организации аналоговых и цифровых каналов по проводным линиям связи и в беспроводных средах, принципов контроля передачи информации, кодирования и сжатия данных, современных технологий организации локальных сетей (Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN), сетевого оборудования локальных сетей.

Для специальности 22.01 настоящее пособие может быть использовано при изучении курсов “Сети и средства телекоммуникаций” и “Администрирование сетевых систем”.

Автор: Брейман А.Д.

Рецензенты: проф., к.т.н. Рощин А.В.
доц., к.т.н. Журавлев В.А.

Работа рассмотрена и одобрена на заседании кафедры ИТ-4 “Персональные компьютеры и сети” 19 апреля 2001г, протокол №11.

Зав. кафедрой ИТ-4,
профессор, д.т.н.

Михайлов Б.М.

© Брейман А.Д., 2001
© МГАПИ, 2001

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	6
1. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕЙ.....	8
1.1. Функциональные возможности сетей.....	8
1.2. Структурная организация компьютерной сети.....	10
1.2.1. Сети разного масштаба.....	10
1.2.2. Среды передачи данных.....	11
1.2.3. Режимы передачи данных.....	11
1.2.4. Способы коммутации.....	12
1.2.5. Организация виртуальных каналов.....	13
2. ОРГАНИЗАЦИЯ СЕТЕВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ....	13
2.1. Архитектура СПО.....	13
2.2. Основные модели взаимосвязи открытых систем.....	14
2.2.1. Эталонная модель ВОС.....	15
2.2.2. Модель ТСР/IP.....	17
3. АНАЛОГОВЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ.....	17
3.1. Аналоговая модуляция.....	17
3.2. Модемы.....	18
3.3. Протоколы, поддерживаемые модемами.....	19
3.4. Режимы передачи.....	20
3.5. Асинхронная, синхронная, изохронная и плезиохронная передача.....	20
4. ЦИФРОВЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ.....	21
4.1. Частотное и временное разделение каналов.....	22
4.2. Проводные линии связи и их характеристики.....	22
4.2.1. Витая пара.....	22
4.2.2. Коаксиальный кабель.....	24
4.2.3. Волоконно-оптический кабель.....	25
4.3. Беспроводные среды передачи данных.....	27
4.3.1. Инфракрасные волны.....	27
4.3.2. Радиоволны, сигналы с узкополосным спектром.....	27
4.3.3. Радиоволны, широкополосные сигналы.....	27
4.3.4. Спутниковая связь.....	29
4.3.5. Сотовая связь.....	30
5. ПЕРЕДАЧА ДАННЫХ И КОДИРОВАНИЕ ИНФОРМАЦИИ.....	31
5.1. Количество информация и энтропия.....	31
5.2. Свойства энтропии.....	33
5.3. Единицы количества информации.....	33
5.4. Качество обслуживания.....	34
5.5. Кодирование информации.....	34
5.6. Логическое кодирование.....	36
5.7. Самосинхронизирующиеся коды.....	39
6. КОНТРОЛЬ ПЕРЕДАЧИ ИНФОРМАЦИИ И СЖАТИЕ ДАННЫХ.....	39
6.1. Самовосстанавливающиеся коды.....	39
6.2. Систематические коды.....	40

6.3. Алгоритмы сжатия данных	40
6.3.1. Алгоритм RLE.....	41
6.3.2. Алгоритм Лемпела-Зива	41
6.3.3. Кодирование Шеннона-Фано	42
6.3.4. Алгоритм Хаффмана	42
7. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ЛОКАЛЬНЫХ СЕТЕЙ.....	43
7.1. Сетевые топологии	43
7.1.1. Шина	44
7.1.2. Дерево	44
7.1.3. Звезда с пассивным центром	44
7.1.4. Звезда с интеллектуальным центром.....	45
7.1.5. Кольцо.....	45
7.1.6. Цепочка.....	46
7.1.7. Полносвязная топология.....	46
7.1.8. Произвольная (ячеистая) топология.....	46
7.2. Методы доступа и их классификация.....	47
7.2.1. Метод доступа с контролем несущей и определением коллизий	48
7.2.2. Маркерные методы доступа	48
8. ТЕХНОЛОГИЯ ETHERNET.....	50
8.1. Стандарты группы IEEE 802.....	50
8.2. Протокол управления логическим каналом IEEE 802.2	51
8.3. Технология Ethernet	53
8.4. Метод доступа CSMA/CD	53
8.5. Время двойного оборота	54
8.6. Форматы кадров Ethernet	54
8.7. Пропускная способность сети Ethernet.....	55
9. СЕТИ TOKEN RING И FDDI.....	56
9.1. Технология Token Ring.....	56
9.1.1. Маркерный метод доступа	56
9.1.2. Система приоритетного доступа.....	60
9.1.3. Оборудование Token Ring	60
9.2. Технология FDDI	61
10. ВЫСОКОСКОРОСТНЫЕ ТЕХНОЛОГИИ ЛОКАЛЬНЫХ СЕТЕЙ	63
10.1. Технология Fast Ethernet 100Мбит/с.....	63
10.2. Технология Gigabit Ethernet 1000 Мбит/с	65
10.3. Технология 100VG-AnyLAN	66
11. СЕТЕВОЕ ОБОРУДОВАНИЕ ЛОКАЛЬНЫХ СЕТЕЙ	67
11.1. Сетевые адаптеры	67
11.2. Концентраторы.....	68
11.3. Мосты.....	69
11.4. Коммутаторы.....	71
11.5. Алгоритм покрывающего дерева	73
СПИСОК ЛИТЕРАТУРЫ.....	75

ВВЕДЕНИЕ

Последнее десятилетие XX века можно с большим основанием назвать десятилетием компьютерных сетей. В коммерческих фирмах и государственных учреждениях, учебных заведениях и даже дома все реже можно встретить компьютеры, никаким образом не связанные с другими. Если для предприятий и организаций наиболее важным оказалось развертывание локальных сетей, то домашних пользователей все больше привлекают глобальные сети - Интернет, иногда FIDO.

Два-три десятилетия назад только крупная организация могла позволить себе приобрести хотя бы один компьютер, потому что он стоил сотни тысяч долларов, требовал много места для размещения, и необходим был квалифицированный, а значит, высокооплачиваемый, обслуживающий персонал. Как правило, компьютеры тогда работали в пакетном режиме, пользователь (обычно программист) мог вообще никогда и не увидеть ЭВМ, выполняющую его задачи. Программы записывались на специальных бланках, по которым операторы готовили перфокарты, наконец, программу в виде колоды перфокарт нужно было отдать системному администратору, который ставил задание в очередь и, после его выполнения, отдавал распечатку с результатами.

Такой режим нельзя назвать удобным (хотя именно в таком режиме эффективность работы компьютера максимальна), и лет через десять появились терминалы – устройства, включавшие в себя дисплей и клавиатуру. Терминал подключался к центральному компьютеру кабелем. Первые терминалы были малоинтеллектуальными, их даже называли 'тупыми' (dumb): все, что они умели делать – это сообщить центральному компьютеру, какая клавиша нажата и, приняв от него управляющую команду, отобразить символ на дисплее. (В качестве терминалов поначалу использовали устройства телексной связи – телетайпы, отсюда и небогатый набор их возможностей.) Чуть позже поняли, что если терминал снабдить своим простеньким процессором и оперативной памятью, то самому центральному компьютеру придется меньше заниматься непродуктивной работой.

Также оказалось удобно, если терминал стоит на столе у человека, который им пользуется, даже если этот стол находится не в том же здании, что и центральный компьютер. Так появились модемы, предоставившие терминалам возможность связываться со своими центральными компьютерами по телефонным сетям.

До сих пор информационные и финансовые агентства (например, Reuter и Bloomberg) предоставляют доступ к своей информации именно с помощью терминалов. Именно из решения проблем связи терминалов с центральными компьютерами и выросла вся индустрия сетей передачи данных.

Терминалы постепенно интеллектуализировались все больше, и наконец переросли в качественно новые устройства – рабочие станции, которые представляли из себя в большой степени независимые компьютеры, однако в полной мере могли выполнять свои функции только при подключении к серверу.

Надо понимать, что на западе до сих пор очень остро стоит проблема 'унаследованных' (inherited) систем: многие крупные организации до сих пор в своей работе используют мэйнфреймы и терминалы, и критическая масса их данных находится именно там. В то же время в России массовая компьютеризация началась в конце 1980-х годов и почти целиком опиралась на IBM PC-совместимые персональные компьютеры. Только в редких крупных организациях необходимость объемных вычислений и/или повышенные требования к надежности приводили к использованию "больших" ЭВМ, таких, как IBM AS/400, различные серверы и рабочие станции фирмы Sun и т.п. Компьютеры же класса IBM System/360 (ЕС ЭВМ), до такой степени распространенные на западе, что фирма Microsoft включила в состав своего пакета серверных приложений BackOffice сервер связи с такими компьютерами (SNA Server), в России практически прекратили существование.

Обычная дорога к сетям для наших организаций и фирм выглядела так: есть несколько IBM PC – совместимых компьютеров. На них вводятся тексты, строятся таблицы, выполняются расчеты. Текстовые файлы, файлы электронных таблиц, рисунков, данные и результаты расчетов постоянно нужно переносить с компьютера на компьютер. Для этого пользуются дискетами. Пока объемы данных невелики, и обрабатывать эти данные можно по очереди, особых проблем не возникает. Однако вскоре появляется желание, например, собрать все данные о продажах в базу данных, и сделать так, чтобы несколько продавцов могли одновременно выписывать счета и фиксировать оплаты товара так, чтобы остальные сразу видели эти новые счета и записи об оплатах. Бегать с дискетой после каждого выписанного счета – нереально. И тут выясняется, что можно приобрести недорогие сетевые карты для каждого из компьютеров, соединить их кабелем, установить специальное сетевое программное обеспечение, и проблема может быть решена. Это путь "от удобства".

Другой путь к сетям лежит "от экономии". Зачем нужно тратить деньги на несколько полноценных компьютеров для машинисток, если можно приобрести один компьютер помощнее, с большим объемом дисковой памяти, несколько машин совсем без жестких дисков, и соединить их в сеть. Тогда более слабые компьютеры смогут пользоваться дисковым пространством более мощного. Вот и экономия – стоимость нескольких жестких дисков заметно больше стоимости требуемого сетевого оборудования. Наконец, путь "от моды". Когда все знакомые, соседи и конкуренты уже поставили себе локальные сети, то, наверное, в этом есть какой-то смысл. И хотя насущной необходимости пока нет, стоит держаться в русле технического прогресса. Как правило, и в этом случае оказывается, что сеть помогает упростить жизнь и приносит пользу.

1. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕЙ

1.1. Функциональные возможности сетей

Польза от использования сетей может относиться к разным категориям.

Во-первых, прямое общение людей (коммуникация). При этом сеть используется как среда, передающая от одного человека другому набранный на клавиатуре текст, введенный с микрофона голос, полученное с видеокамеры изображение или и то, и другое, и третье. Сюда относятся электронная почта, различные системы для разговоров (чат-системы), системы типа ICQ, Internet Phone, видеоконференции, и многое другое. Естественно, для этого используется программное обеспечение, но оно играет чисто техническую роль приемопередатчика, подобно телефонному аппарату при разговоре по телефону.

Во-вторых, передача данных между программами и людьми. При этом на одной стороне информационного потока находится программный процесс, например, Система Управления Базами Данных (СУБД), а на другой – человек-пользователь. Человек, конечно, использует программы для доступа к СУБД, но эти программы так же, как в первом случае, играют чисто техническую роль. Однако СУБД уже выступает как полноправный участник передачи данных. Другим примером может служить сетевая файловая система, обеспечивающая доступ к файлам на другом компьютере. Такие программы, которые выполняют некоторые действия по собственной инициативе, а не по прямой команде от пользователя, будем называть активными программами или программными агентами.

В-третьих, передача данных между активными программами. В этом случае человек явно не участвует в процессе передачи данных. Например, система зеркалирования содержимого узлов Интернета, может выполняться автоматически через заданные промежутки времени или в соответствии с другими критериями. Надо понимать, что, в конце концов, результатами функционирования таких программ все равно будет пользоваться человек, и только ради этого они и созданы и запущены.

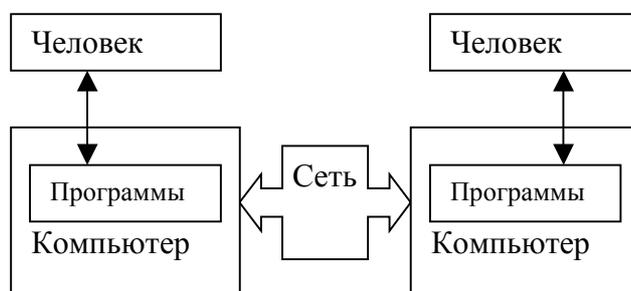


Рис. 1.1

Отношения "человек-программа" функционально асимметричны: человек является либо поставщиком данных, либо их пользователем. Программы же либо просто хранят, либо преобразуют хранимую информацию.

Отношения сети и компьютера тоже асимметричны. Если компьютер может работать без сети, автономно, то сеть без компьютеров немыслима.

Определимся, что же такое компьютерная сеть. Под компьютерной сетью принято понимать совокупность компьютеров, соединяющих их каналов связи и дополнительного оборудования, предназначенная для обмена данными.

Тогда схема рис.1.1. немного преобразуется:

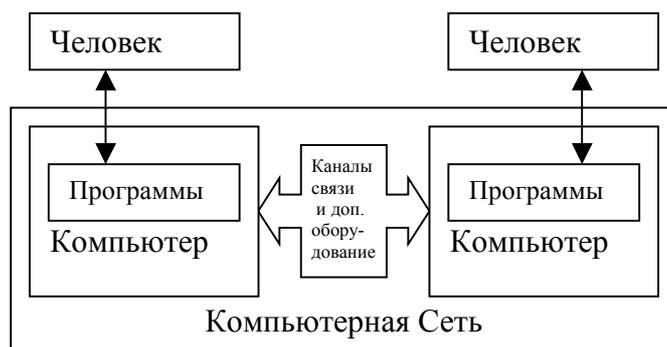


Рис.1.2

Рассмотрим по порядку, какими свойствами должна обладать компьютерная система, чтобы называться сетью.

Во-первых, для сети нужны компьютеры – как минимум, два. Будем называть эти компьютеры – узлами сети, или просто **узлами**. Можно также встретить термины "**станция данных**", "**оконечная система**". Принципиальных ограничений сверху на количество компьютеров в сети нет (однако для любой конкретной сетевой технологии такие ограничения всегда есть – либо ограничивается общее количество компьютеров, либо количество сегментов сети и компьютеров в них). Сети принято классифицировать не столько по размеру (количеству узлов), сколько по масштабу (охватываемой территории) – локальные, региональные и т.д.

Во-вторых, компьютеры должны быть соединены **каналами передачи данных** (КПД). Канал передачи данных состоит из **линии передачи данных** (ЛПД) и **аппаратуры окончания канала данных** (АОКД). За последним термином скрываются такие устройства, как, например, модем или сетевая карта. Для обозначения АОКД будем пользоваться современным термином "**сетевой интерфейс**". Часто для обеспечения функционирования сети оказывается необходимым использовать дополнительное оборудование – повторители, мосты, коммутаторы, маршрутизаторы и пр. Совокупность каналов передачи данных и дополнительного сетевого оборудования называется **сетью передачи данных** (СПД).

В-третьих, компьютеры должны быть оснащены сетевым программным обеспечением (СПО) – как правило, сетевой операционной системой (СОС) или сетевой надстройкой над обычной операционной системой. СПО, установлен-

ное на разных компьютерах может быть разным, но обязательно совместимым друг с другом – то есть реализовывать один набор протоколов передачи данных.

В-четвертых, хотя бы один компьютер должен предоставлять для общего пользования часть своих ресурсов – дисковое пространство, принтер, программы и т.д. Такой компьютер называется **сервером**. Кроме этого, все остальные узлы сети (клиенты), должны иметь возможность использовать ресурсы серверов. Ресурсы, предоставляемые в общее пользование сервером, будем называть **разделяемыми ресурсами**.

Четвертое свойство не всегда очевидно (например, в случае сети, используемой только для обмена электронной почтой, сложно выделить разделяемые ресурсы), однако обязательно присутствует (такими ресурсами для примера с электронной почтой могут выступать программа почтового сервера, дисковое пространство, отведенное для хранения сообщений, процессорное время, затрачиваемое на обработку почты).

В большинстве случаев, название разделяемого ресурса указывается в названии сервера: файловый сервер (ресурс – дисковые файлы), сервер печати (ресурс – принтеры), сервер приложений (ресурс – прикладные программы), сервер баз данных (ресурс – базы данных) и т.д.

Отметим, что перечисленные свойства отражают разные аспекты сущности компьютерной сети. Первые два свойства можно назвать структурными – они определяют, из каких элементов состоит сеть и как эти элементы связаны между собой. Третье свойство – программное, указывающее на необходимость специальных программ, без которых элементы сети останутся разобщенными, даже будучи физически связанными. Наконец, четвертое свойство – прагматическое, оно содержит указание на то, что цель создания сети лежит не в ней самой, а той пользе, которую сеть может принести.

1.2. Структурная организация компьютерной сети

1.2.1. Сети разного масштаба

Организация сети и ее структура непосредственно зависят от используемых компьютеров и расстояний между ними. Наиболее очевидны различия в организации сетей разных масштабов. Принято различать сети:

- локальные (комната, здание, комплекс зданий),
- городские (район города, город),
- региональные (область, страна, континент),
- глобальные (планета).

Для сетей разных масштабов свойственны разные способы организации. Причин тому несколько, среди них на первом месте стоит качество линии передачи данных, обусловленное ограниченностью скорости передачи сигнала, отношением сигнал/шум и т.д. В результате с увеличением масштаба сети диапазон используемых скоростей передачи смещается вниз. Кроме того, в случае, например, локальных сетей, запас скорости передачи данных позволяет исполь-

зовать такие варианты организации и режимов работы сети, которые вряд ли могли бы применяться в глобальных сетях. Так, из двух основных режимов передачи данных – вещательного и "точка-точка", первый широко используется в локальных сетях, а второй – в глобальных.

1.2.2. Среды передачи данных

Передача данных может происходить по кабелю (в этом случае говорят об ограниченной или кабельной среде передачи) и с помощью электромагнитных волн той или иной природы – инфракрасных, микроволн, радиоволн, – распространяющихся в пространстве (неограниченная среда передачи, беспроводные сети).

В большинстве случаев кабельные среды удобнее, надежнее и выгоднее неограниченных. Как правило, кабель и сопутствующее сетевое оборудование стоит гораздо дешевле оборудования для беспроводных сетей, а скорость передачи данных по кабелю выше. Тем не менее, в некоторых случаях прокладка кабеля либо технически затруднена (например, водные преграды), либо экономически неоправдана (стоимость прокладки кабеля высока, а большая скорость передачи не требуется), либо сталкивается с организационными или иными проблемами (например, необходимо проложить траншею через оживленную магистраль в центре города, на что очень сложно получить согласие городских властей). Кроме того, может появиться необходимость подключения к сети пользователей, по роду деятельности часто меняющих местонахождение (например, кладовщики на большом складе). Во всех подобных (и многих других) случаях могут использоваться беспроводные сети.

Кабельные среды по используемому материалу делятся на “медные” (в самом деле, проводящие жилы таких кабелей могут содержать не только медь, но и другие металлы и их сплавы) и оптические (оптоволоконные, проводящая жила изготавливается из оптически прозрачных материалов – кварца или полимеров). Медные кабели бывают симметричными (все проводники одинаковы, например, витая пара проводников) и асимметричными (например, коаксиальный кабель, состоящий из изолированных друг от друга центральной жилы и оплетки). Оптические кабели различаются по соотношению между толщиной проводящей жилы и несущей частотой передачи данных. Тонкие жилы, диаметр сечения которой сравним с длиной волны несущей частоты, образуют одномодовые кабели (типичная толщина 8-10 мкм), а более толстые – многомодовые (до 50-60 мкм).

При построении беспроводных сетей, как правило, применяется одна из трех технологий: передача в инфракрасном диапазоне, передача данных с помощью узкополосных радиосигналов и передача данных с помощью радиосигналов с распределенным спектром.

1.2.3. Режимы передачи данных

Сети делятся на два класса, различающиеся способом использования канала передачи данных: сети с селекцией данных и маршрутизацией данных.

В сетях с **селекцией данных** существует общий канал передачи, к которому подключены все узлы. В каждый момент времени каналом владеет только один узел, который выдает данные в канал. Любой выданный в канал блок данных получают (в виде копий) все узлы сети. Каждый узел проверяет адрес получателя, переданный с блоком данных, и, сравнив его с собственным адресом, в случае совпадения обрабатывает полученные данные, а в случае несовпадения – отбрасывает их (уничтожает свою копию).

Сети с **маршрутизацией данных** состоят из множества отдельных каналов, соединяющих пары узлов сети. Пара узлов, обладающая общим каналом, может передавать данных друг другу независимо от остальных узлов сети. Для передачи данных между узлами, не имеющими общего канала, необходимо задействовать одного или несколько других узлов, которые осуществили бы маршрутизацию передаваемой информации.

1.2.4. Способы коммутации

Коммутация является необходимым элементом связи узлов между собой, позволяющим сократить количество необходимых линий связи и повысить загрузку каналов связи. Практически невозможно предоставить каждой паре узлов выделенную линию связи, поэтому в сетях всегда применяется тот или иной способ коммутации абонентов, использующий существующие линии связи для передачи данных разных узлов.

Коммутируемой сетью называется сеть, в которой связь между узлами устанавливается только по запросу.

Абоненты соединяются с коммутаторами выделенными (индивидуальными) линиями связи. Линии связи, соединяющие коммутаторы, используются абонентами совместно.

Коммутация может осуществляться в двух режимах: динамически и статически. В первом случае коммутация выполняется на время сеанса связи (обычно от секунд до часов) по инициативе одного из узлов, а по окончании сеанса связь разрывается. Во втором случае коммутация выполняется обслуживающим персоналом сети на значительно более длительный период времени (несколько месяцев или лет) и не может быть изменена по инициативе пользователей. Такие каналы называются **выделенными** (dedicated) или **арендуемыми** (leased).

Две группы способов коммутации: **коммутация каналов** (circuit switching) и **коммутация с промежуточным хранением** (store-and-forward). Вторая группа состоит из двух способов: **коммутации сообщений** (message switching) и **коммутации пакетов** (packet switching).

При коммутации каналов между узлами, которым необходимо установить связь друг с другом, обеспечивается организация непрерывного составного канала, состоящего из последовательно соединенных отдельных каналов между узлами. Отдельные каналы соединяются между собой коммутирующим обо-

дованием (коммутаторами). Перед передачей данных необходимо выполнить процедуру установления соединения, в процессе которой создается составной канал.

Под коммутацией сообщений понимается передача единого блока данных между узлами сети с временной буферизацией этого блока каждым из транзитных узлов. Сообщением может быть текстовый файл, файл с графическим изображением, электронное письмо – сообщение имеет произвольный размер, определяемый исключительно его содержанием, а не теми или иными технологическими соображениями.

При коммутации пакетов все передаваемые пользователем данные разбиваются передающим узлом на небольшие (до нескольких килобайт) части – **пакеты** (packet). Каждый пакет снабжается заголовком, в котором указывается, как минимум, адрес узла-получателя и номер пакета. Передача пакетов по сети происходит независимо друг от друга. Коммутаторы такой сети имеют внутреннюю буферную память для временного хранения пакетов, что позволяет сглаживать пульсации трафика на линиях связи между коммутаторами. Пакеты иногда называют **дейтаграммами** (datagram), а режим индивидуальной коммутации пакетов – **дейтаграммным режимом**.

Сеть с коммутацией пакетов замедляет процесс взаимодействия каждой конкретной пары узлов, поскольку их пакеты могут ожидать в коммутаторах, пока передадутся другие пакеты. Однако общая эффективность (объем передаваемых данных в единицу времени) при коммутации пакетов будет выше, чем при коммутации каналов. Это связано с тем, что трафик каждого отдельного абонента носит пульсирующий характер, а пульсации разных абонентов, в соответствии с законом больших чисел, распределяются во времени, увеличивая равномерность нагрузки на сеть.

1.2.5. Организация виртуальных каналов

В отличие от дейтаграммного режима передачи, предполагающего независимую маршрутизацию каждого пакета, режим **виртуального канала** (virtual circuit или virtual channel) устанавливает единый маршрут для всех пакетов в рамках одного соединения. Перед тем, как начать передачу, передающий узел выдает в сеть специальный пакет – запрос на установление соединения. Этот пакет, проходя через коммутаторы, “прокладывает” виртуальный канал – коммутаторы запоминают маршрут для данного соединения, и последующие пакеты будут отправлены по нему же. При этом время, затраченное на установление виртуального канала, компенсируется более быстрой передачей потока пакетов за счет того, что коммутаторы не выполняют полную маршрутизацию каждого пакета, а быстро определяют его маршрут по номеру виртуального канала.

2. ОРГАНИЗАЦИЯ СЕТЕВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1. Архитектура СПО

Наиболее существенным отличительным признаком сетевого программного обеспечения (СПО) является его принципиально распределенный характер: различные компоненты должны выполняться на разных компьютерах. Из этого следует, что процессы, находящиеся в разных адресных пространствах на разных компьютерах, вынуждены обмениваться данными, не используя привычные средства – общие области памяти и т.п.

Как правило, в СПО можно выделить группы модулей, отвечающих за выполнение различных подзадач: передачу данных по КПД, управление сетевыми адресами, управление пользователями и др. Для упрощения разработки и документирования СПО создан ряд моделей, представляющих разные точки зрения на то, из каких частей состоит СПО, и как они взаимодействуют между собой.

Базовым понятием для всех используемых моделей является понятие протокола. Под **протоколом** (protocol) понимается формально описанный набор правил, определяющий последовательность и формат сообщений, которыми обмениваются сетевые компоненты. Каждая модель, в соответствии с разновидностями выполняемых протоколами функций, выделяет группы протоколов, называемые **уровнями** (level), и описывает взаимосвязь уровней.

Общий подход, разделяемый всеми моделями, состоит в иерархическом упорядочении уровней. То есть, протоколы каждого уровня базируются на использовании протоколов группы, следующей по иерархии. Полный набор протоколов, включающий в себя протоколы всех уровней модели, обычно называется **стеком протоколов** (protocol stack).

Каждый уровень взаимодействует с соседними уровнями формально описанным способом. Говорят, что определен **интерфейс** (interface) между двумя уровнями. Интерфейс определяет набор **услуг, служб** или **сервисов** (service), которые нижележащий уровень предоставляет вышележащему. Каждый уровень состоит из **сущностей** (entities), выполняющих некие действия или **активности** (activities). Для получения услуги вышележащий уровень обращается к **точке доступа к сервису** (service access point, SAP).

По типу различаются службы **с установлением соединения** (connection) и **без соединения** (connectionless). Службы с установлением соединения позволяют сущностям передавать и принимать потоки данных произвольного объема, предварительно договорившись об этом (установив соединение). Службы без соединения передают данные отдельными блоками, независимо один от другого.

Каждая служба состоит из элементарных служб – **примитивов** (primitive). Например, служба передачи файлов может включать примитивы показа списка файлов в текущем каталоге, смены текущего каталога, передачи указанного файла и т.д.

2.2. Основные модели взаимосвязи открытых систем

Международная организация по стандартизации (МОС, International Standardization Organization, ISO) предложила в 1978 г. эталонную **модель взаимо-**

действия открытых систем (ВОС, Open System Interconnect, OSI). На основе этой модели был разработан стек протоколов, не получивший широкого распространения, хотя он и был принят в качестве национального стандарта правительством США еще в 1990 году (проект GOSIP). Тем не менее, модель OSI является главной методологической основой для анализа и разработки сетей.

Стандартом де-факто для глобальных сетей в настоящее время является стек протоколов TCP/IP, разработанный в середине 70-х годов по заказу Министерства обороны США. Позднее была выработана и модель TCP/IP.

В локальных сетях, наряду с TCP/IP, применяются стеки IPX/SPX, Net-BIOS/SMB, XNS, DECnet и другие.

Различия между моделями ВОС и TCP/IP происходят из различных целей и методологий разработки протоколов и услуг. Разработка модели OSI была направлена на довольно амбициозную цель – установление механизмов для распределенной обработки данных в аппаратно и программно разнородных компьютерных средах. Цели разработки протоколов TCP/IP были гораздо скромнее и прагматичнее: установление механизмов для соединения сетей и предоставление пользователям этих сетей набора базовых коммуникационных услуг.

Разработкой протоколов ВОС занималась крупная международная организация – МОС. Подобным организациям свойственно замедленное функционирование. Работа над стандартами ВОС показала как недостаточную мобильность таких организаций перед лицом предельно интенсивного технологического развития в данной области, как и сложности с установлением баланса зачастую противоречивых интересов многих участников работы.

Разработка протоколов TCP/IP происходила в среде, ориентированной на практическое применение. В центре внимания были конкретные проблемы, касающиеся связи сетей и обслуживания пользователей. Разработку TCP/IP начинали ради решения проблем сети ARPANET – в первую очередь, взрывного роста количества подключенных компьютеров и, соответственно, трафика, ими производимого. Протокол IP должен был предоставить средства разделения единой сети, которой была ARPANET, на множество подсетей, изолирующих внутренний трафик друг от друга. Нужно было создать сеть сетей вместо сети компьютеров.

2.2.1. Эталонная модель ВОС

При разработке модели ВОС выделение уровней базировалось на следующих принципах:

- каждый уровень должен выполнять отдельную функцию,
- поток информации между уровнями должен быть минимизирован,
- функции уровней должны быть удобны для определения международных стандартов,
- количество уровней должно быть достаточным для разделения функций, но не избыточным.

Модель ВОС определяет семь уровней: физический, канальный, сетевой, транспортный, сеансовый, представления данных, прикладной.

Физический уровень (Physical layer) – организует передачу битов по КПД. Стандарты этого уровня определяют характеристики кабелей и разъемов, схемы кодирования электрического или оптического сигнала и прочие параметры КПД.

Канальный уровень (Data link layer) – обеспечивает надежную доставку данных в физической сети. Стандарты этого уровня определяют правила совместного использования КПД и делятся на две группы: подуровень **управления логическим каналом** (Logical Link Control – LLC) и подуровень **управления доступом к среде** (Medium Access Control – MAC). Поток битов между двумя участниками сети делится на **кадры** (frame), и канальный уровень гарантирует безошибочную доставку кадров. Кроме того, канальный уровень решает, кто из участников может передавать данные в каждый момент времени, управляет потоком данных (буферизацией) и контролирует последовательность кадров.

Сетевой уровень (Network layer) – обеспечивает передачу данных между сетями. На этом уровне находятся системы адресации участников сетей и системы маршрутизации. Сетевой уровень выбирает способ передачи данных по сети: это может быть как коммутация каналов, так и коммутация пакетов. В сетях с коммутацией пакетов сетевой уровень делит поток данных на пакеты, независимо маршрутизируемые по сети. Пакеты могут передаваться как по виртуальным каналам, так и в виде дейтаграмм.

Транспортный уровень (Transport layer) – представляет собой интерфейс пользовательской системы с сетью передачи данных. Он отвечает за надежную передачу данных и распределение обязанностей между участниками сети.

Сеансовый уровень (Session layer) – предназначен для организации диалога между процессами. Основные функции уровня – обработка подключений (login) и отключений (logout), аутентификация, синхронизация.

Уровень **представления данных** (Presentation layer) – управляет представлением информации в сети. Гарантирует, что данные, которыми обмениваются участники, записаны в формате, которых понимают обе стороны. Уровень имеет дело с наборами символов (character sets), форматами данных, кодированием и упаковкой данных.

Прикладной уровень (Application layer) – это интерфейс между сетью и пользовательскими программами. Типичные услуги, предоставляемые прикладным уровнем – электронная почта, передача файлов и т.д.

2.2.2. Модель TCP/IP

В отличие от модели ВОС, разработка которой велась под сильным влиянием телекоммуникационных компаний, исходя из соображений международной совместимости, модель TCP/IP была создана уже после разработки протоколов и отражала в основном свойства именно этого стека протоколов.

Модель включает сетевой, межсетевой, транспортный и прикладной уровни.

Сетевой уровень (Network layer) – соответствует канальному уровню ISO.

Межсетевой уровень (Internet layer) – соответствует сетевому уровню ISO.

Транспортный уровень (Transport layer) – соответствует транспортному (и части сеансового) уровня ISO.

Прикладной уровень (Application layer) – включает все уровни ISO, выше транспортного.

Детальное описание протоколов TCP/IP будет приведено во второй части настоящего пособия.

3. АНАЛОГОВЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ

Под **каналом передачи данных** (КПД) понимается совокупность среды передачи (среды распространения сигнала) и технических средств передачи между канальными интерфейсами. В зависимости от формы информации, которую может передавать канал, различают **аналоговые** и **цифровые** каналы.

Аналоговый канал на входе (и, соответственно, на выходе) имеет непрерывный сигнал, те или иные характеристики которого (например, амплитуда или частота) несут передаваемую информацию. Цифровой канал принимает и выдает данные в цифровой (дискретной, импульсной) форме.

3.1. Аналоговая модуляция

Поскольку сети связывают цифровые компьютеры, по каналу связи необходимо передавать дискретные данные. Соответственно, при использовании аналоговых сигналов необходимо некоторое преобразование (кодирование) передаваемых данных этими сигналами. Такое преобразование называется **аналоговой модуляцией** (или аналоговым кодированием). В его основе лежит изменение одной из характеристик синусоидального несущего сигнала в соответствии с последовательностью передаваемых данных. Основные способы аналоговой модуляции: амплитудная, частотная и фазовая. Возможно также использование комбинированных методов, например, сочетания амплитудной и фазовой модуляций.

При **амплитудной** модуляции изменяется только амплитуда синусоиды несущей частоты, при передаче логической единицы выдается синусоида одной амплитуды, а при передаче логического нуля – другой амплитуды. Этот способ в чистом виде обладает низкой помехоустойчивостью и применяется редко.

При **частотной** модуляции изменяется только частота несущей – для логической единицы и логического нуля выбираются синусоиды двух различных частот. Этот способ достаточно просто реализуем, и часто применяется при низкоскоростной передаче данных.

При **фазовой** модуляции логической единице и логическому нулю соответствуют сигналы одинаковой амплитуды и частоты, но отличающиеся по фазе (например, 0 и 180 градусов).

Из комбинированных методов широко используются методы **квадратурной амплитудной модуляции** (Quadrature Amplitude Modulation, QAM), сочетающие амплитудную модуляцию с 4 уровнями амплитуды и фазовую модуляцию с 8 значениями сдвига фазы. Из 32 возможных комбинаций амплитуды и сдвига фазы для передачи данных в разных модификациях метода используются всего несколько, в то время, как все остальные комбинации являются запрещенными, что позволяет улучшить распознавание ошибочных сигналов.

3.2. Модемы

Устройства, выполняющие модуляцию и демодуляцию (восстановление из модулированного сигнала исходных данных), называются **модемами** (МО-Дулятор-ДЕМОдулятор). Модемы классифицируют по области применения, функциональному назначению, типу используемого канала, поддержке протоколов модуляции, исправления ошибок и сжатия данных, конструктивному исполнению.

По области применения модемы можно разделить на следующие группы:

- для коммутируемых телефонных каналов,
- для выделенных каналов,
- для физических линий:
 - узкополосные (baseband),
 - короткого радиуса действия (short range или line driver),
- для цифровых систем передачи (CSU/DSU),
- для сотовых систем связи,
- для радиоканалов с пакетной передачей,
- для локальных радиосетей.

Модемы для коммутируемых телефонных каналов предназначены для широкого круга пользователей и наиболее распространены. Такие модемы должны работать в полосе пропускания 3,1 кГц в голосовом диапазоне (поскольку аппаратура АТС не пропустит другие сигналы), уметь взаимодействовать с АТС – набирать номер в импульсном или тоновом режиме, определять сигнал “занято” и т.д.

Модемы для выделенных арендованных каналов отличаются от модемов для коммутируемых линий только в том, что им не требуется взаимодействовать с аппаратурой АТС для установления соединения. Они тоже должны работать в узкой полосе пропускания.

Модемы для физических линий не ограничены узкой полосой пропускания, определенной АТС (при этом действуют другие ограничения полосы, свя-

занные с длиной, экранированностью и другими характеристиками линии). Узкополосные модемы для физических линий используют методы модуляции, аналогичные применяемым в модемах для коммутируемых линий, но за счет более широкой полосы пропускания, могут достигать более высоких скоростей передачи – 128 Кбит/с и выше.

Модемы короткого радиуса действия используют уже не аналоговую модуляцию, а цифровые сигналы. Часто используются разнообразные методы цифрового кодирования, исключаяющие постоянную составляющую из сигнала.

Модемы для цифровых систем передачи обеспечивают подключение к стандартным цифровым каналам (T1/E1, ISDN) и поддерживают функции канальных интерфейсов.

Модемы для сотовых систем связи обычно поддерживают специальные протоколы модуляции и коррекции ошибок, позволяющие работать при часто изменяющихся параметрах среды передачи и высоком уровне помех.

Модемы для радиоканалов с пакетной передачей используют одну и ту же полосу частот, в которой организуется множественный доступ, например, с контролем несущей. Достижимая при этом скорость передачи обычно невысока – до 64 Кбит/с, но расстояние между станциями может составлять несколько километров.

Модемы для локальных радиосетей обеспечивают передачу данных с высокой скоростью (до 16 Мбит/с) на небольшие расстояния (до 300 м). Для предотвращения взаимного влияния нескольких одновременно передающих модемов используются различные способы, например, псевдослучайной перестройки рабочей частоты или широкополосной передачи.

По методу передачи модемы обычно делят на синхронные и асинхронные. Поскольку модем связан, с одной стороны, с компьютером, а с другой стороны – через канал – с другим модемом, возможен асинхронно-синхронный режим работы: модем получает данные от компьютера асинхронно, а передает их другому модему в синхронном режиме.

3.3. Протоколы, поддерживаемые модемами

Все модемные протоколы можно разделить на международные и фирменные. Часто фирменный протокол, разработанный той или иной компанией, реализуют и другие производители модемов, он становится стандартом де-факто, а затем на его основе вырабатывается международный стандарт.

Международные стандарты в области электросвязи выпускаются Комитетом по стандартизации коммуникаций ИТУ-Т (ранее называвшейся Международным консультативным комитетом по телефонии и телеграфии, МККТТ – Comitet Consultatif Internationale de Telegraphique et Telephonique, ССИТТ) в форме рекомендаций. Рекомендации ИТУ-Т, касающиеся модемов, относятся к серии V.

Модемные протоколы можно разбить на несколько групп:

- протоколы, определяющие соединение модема и канала связи: V.2, V.25 и др.

- протоколы, определяющие соединение модема с ООД (компьютером): V.10, V.11, V.14, V.25, V.25bis, V.28 и др.
- протоколы модуляции: V.17, V.22, V.32, V.32bis, V.32ter, V.34, V.90, HST, PER, ZyX и др.
- протоколы коррекции ошибок: MNP1-MNP4, MNP6, MNP10, V.41, V.42;
- протоколы сжатия данных: V.42bis, MNP5, MNP7;
- протоколы согласования параметров связи: V.8;
- протоколы диагностики модемов: V.51-V.54, V.56.

3.4. Режимы передачи

Режим передачи определяет способ коммуникации между двумя узлами. При **симплексном** (simplex) режиме приемник и передатчик связывается линией связи, по которой информация передается только в одном направлении. Передающий узел в симплексном режиме полностью занимает канал. Примеры: радиовещание, телевидение.

Полудуплексный (half duplex) режим допускает передачу в двух направлениях, но в разные моменты времени. Два узла связываются таким каналом связи, который позволяет им поочередно (но не одновременно) передавать информацию. Для смены направления передачи, как правило, используется передача специального сигнала и получение подтверждения.

Дуплексный или **полнодуплексный** (duplex, full duplex) режим позволяет одновременно передавать информацию в двух направлениях. В простейшем случае для дуплексной связи используется две линии связи (прямая и обратная), но существуют решения, позволяющие поддерживать дуплексный режим на единственной линии (например, оба узла могут одновременно передавать данные, а из принимаемого сигнала вычитать собственные данные). Дуплексный режим может быть симметричным (полоса пропускания канала одинакова в обоих направлениях) или асимметричным.

3.5. Асинхронная, синхронная, изохронная и плезиохронная передача

Для последовательной передачи данных достаточно одной линии, по которой могут последовательно передаваться биты данных. Приемник должен уметь распознавать, где начинается и где заканчивается сигнал, соответствующий каждому биту данных. Другими словами, передатчик и приемник должны уметь синхронизироваться. Если качество синхронизации низкое (за время передачи одного бита рассогласование достигает нескольких процентов), используется **асинхронный** (asynchronous) режим: выполняется согласование синхрогенераторов в начале передачи каждого байта. Как правило, передача байта начинается со специального старт-бита, затем следуют биты данных, а за ними, возможно, бит четности. После всех битов данных передается стоп-бит. Сарт-бит и стоп-бит всегда имеют определенное значение: старт-бит кодируется логическим нулем, а стоп-бит – логической единицей. Между передачей стоп-бита одного байта и старт-бита следующего байта может проходить произволь-

ное время. Асинхронный режим сильно зависит от погрешностей синхрогенераторов, задающий моменты приема битов. Чем выше скорость передачи, тем больше эта погрешность. В результате этих и некоторых других ограничений скорость передачи в асинхронном режиме ограничена сотнями килобит в секунду (стандартные скорости: 50, 75, 110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 бит/с).

Если синхронизация очень качественная (например, используется дополнительная линия, по которой передаются синхросигналы), то можно передавать поток данных без дополнительной синхронизации отдельных байтов. Такой режим называется **синхронным** (synchronous). Передача битов данных предваряется и заканчивается выдачей в канал символа синхронизации. При отсутствии данных передатчик должен постоянно передавать в канал символы синхронизации.

В случае **изохронной** (isochronous) передачи отправка кадров данных происходит в заданные (известные приемнику и отправителю) моменты времени. При этом данные, передаваемые одним узлом с постоянной скоростью, будут поступать к приемнику с той же скоростью. Isochronous передача необходима, например, для доставки оцифрованного видеоизображения или звука.

Плезиохронная (plesiochronous) передача требует внутренней синхронизации узлов от источников с номинально совпадающими частотами. Термин “плезиохронная” означает “почти синхронная”, поскольку частоты источников точно не совпадают, и со временем накапливается расхождение, которое компенсируется вставкой фиктивных данных.

4. ЦИФРОВЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ

Биты данных могут передаваться в виде аналоговых или цифровых сигналов. Для передачи информации обычно используется одна из характеристик сигнала: амплитуда, частота, фаза. При использовании аналоговых сигналов, характеристика (например, амплитуда) может принимать любое значение из некоторого непрерывного интервала. При использовании цифровых сигналов, характеристика может принимать значения только из некоторого конечного набора (в простейшем случае, одно из двух значений).

На этом уровне вместо битовой скорости (бит/с) используют понятие скорости изменения сигнала в линии или бодовой скорости (бод, baud). Эта скорость представляет собой число изменений различаемых состояний линии за единицу времени. В случае двухуровневого кодирования битовая и бодовая скорости совпадают, но с увеличением количества различимых уровней, битовая скорость растет, а бодовая остается постоянной.

Передача данных может происходить по кабелю (в этом случае говорят об ограниченной среде передачи и проводных линиях связи) и с помощью электромагнитных волн той или иной природы – инфракрасных, микроволн, радиоволн, – распространяющихся в пространстве (неограниченная среда передачи, беспроводные линии связи).

4.1. Частотное и временное разделение каналов

Коммутаторы должны обеспечивать использование соединяющих их каналов для одновременной передачи нескольких абонентских составных каналов. Для этого применяются разнообразные техники мультиплексирования абонентских каналов, среди которых **частотное мультиплексирование** (FDM, Frequency Division Multiplexing) и **мультиплексирование с разделением времени** (TDM, Time Division Multiplexing, или **синхронный режим передачи** – STM, Synchronous Transfer Mode).

Частотное мультиплексирование сводится к разделению диапазона частот на полосы, каждая из которых отведена для передачи данных одного абонентского канала. Коммутатор выполняет перенос частоты каждого канала в выделенную для него полосу (обычно путем модуляции высокочастотной несущей низкочастотным сигналом данных).

При мультиплексировании с разделением времени мультиплексор в каждый момент времени выдает в общий канал данные единственного абонентского канала, отдавая ему всю полосу пропускания, но чередуя абонентские каналы через равные промежутки времени. Мультиплексирование с разделением времени ориентировано на дискретный характер передаваемых данных и цифровые каналы.

4.2. Проводные линии связи и их характеристики

Для соединения компьютеров в локальную сеть обычно используют металлические (преимущественно медные) витые пары и коаксиальные кабели. Все более широкое распространение приобретают волоконно-оптические кабели.

4.2.1. Витая пара

В настоящее время среди сетевых кабелей наиболее распространена витая пара, представляющая собой пару переплетенных проводов. При этом вряд ли вы получите работающую витую пару, взяв два любых провода и несколько раз перекрутив их между собой. Для обеспечения требуемой скорости передачи данных по витой паре, она должна удовлетворять стандартам на площадь поперечного сечения провода, на количество витков на единицу длины и на расстояние от последнего витка до разъема.

Существует две разновидности витой пары: экранированная (STP, Shielded Twisted Pair) и неэкранированная (UTP, Unshielded Twisted Pair). В основном используется более удобная при монтаже и дешевая неэкранированная витая пара. В 1991 году был разработан стандарт EIA/TIA-568 (“Стандарт телекоммуникационных кабельных систем для коммерческих зданий”) и близкий к нему международный стандарт ISO/IEC 11801, определяющие для кабелей UTP пять категорий (волновое сопротивление кабеля любой категории – 100 Ом):

- категория 1 (CAT 1) применяется для передачи голоса и низкоскоростной передачи данных (до нескольких десятков Кбит/с);
- категория 2 (CAT 2) использовалась в кабельных системах IBM и гарантировали полосу пропускания 1 МГц;
- категория 3 (CAT 3) применяется для передачи голоса и данных со скоростью до 16 Мбит/с (полоса пропускания 16 МГц);
- категория 4 (CAT 4) представляет собой улучшенный вариант CAT 3: повышена помехоустойчивость, уменьшено затухание сигнала, полоса пропускания расширена до 20 МГц;
- категория 5 (CAT 5) специально предназначена для высокоскоростной передачи данных (100 Мбит/с), обладает полосой пропускания 100 МГц.

Выпускаются кабели категорий, не входящих в стандарт: 6 и 7, обладающими полосами пропускания 200 МГц и 600 МГц. При прокладке новых кабельных систем обычно используют именно кабель CAT 5, даже в том случае, если переход к высокопроизводительным сетям пока не планируется.

Новая редакция стандарта EIA/TIA-568A не включает категории 1 и 2.

Кабели UTP выпускаются преимущественно в 4-х парном исполнении (рис. 4.1), иногда встречаются 2-х парные кабели, обычно CAT 3, и многопарные кабели – 25 пар и более. Основные сетевые технологии – Ethernet и Token Ring – используют только две пары, но существуют и технологии (100VG-AnyLAN), передающие данные по всем четырем парам. Пары помечены цветом изоляции: синий и бело-синий, оранжевый и бело-оранжевый, зеленый и бело-зеленый, коричневый и бело-коричневый.

Для соединения кабелей и оборудования используются 8-контактные разъемы RJ-45 (рис. 4.2). Стандарт EIA/TIA-568A определяет два варианта раскладки проводников по контактам: T568A (табл. 4.1) и T568B (табл. 4.2). В каждой локальной сети может использоваться любой вариант разводки, но не оба сразу.

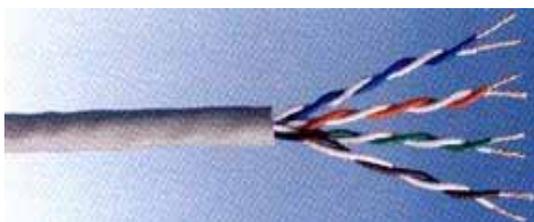


Рис. 4.1. 4-парный кабель UTP



Рис. 4.2. Разъем RJ-45

Раскладка T568A		
Контакт	Цвет	Пара
1	Бело-зеленый	3
2	Зеленый	3
3	Бело-оранжевый	2
4	Синий	1
5	Бело-синий	1
6	Оранжевый	2
7	Бело-коричневый	4
8	Коричневый	4

Табл. 4.1

Раскладка T568B		
Контакт	Цвет	Пара
1	Бело-оранжевый	2
2	Оранжевый	2
3	Бело-зеленый	3
4	Синий	1
5	Бело-синий	1
6	Зеленый	3
7	Бело-коричневый	4
8	Коричневый	4

Табл. 4.2.

Витая пара используется для передачи данных на расстояния до нескольких сотен метров. Стандарт Ethernet ограничивает длину сегмента на неэкранированной витой паре до 100 м. (Некоторые фирмы, например 3COM, выпускают сетевое оборудование в этом стандарте, позволяющее увеличить длину сегмента почти до 200 м.)

Основной недостаток неэкранированной витой пары – сильная подверженность влиянию электромагнитных помех.

Экранированная витая пара (STP) хорошо защищает передаваемые сигналы от влияния внешних электромагнитных полей, но требует заземления экрана при проводке, что усложняет и удорожает кабельную систему. Кабель STP в основном используется фирмой IBM, которая фирменным стандартом определила девять его категорий – от Type 1 до Type 9. Кабель Type 1 состоит из двух пар и по параметрам близок к UTP CAT 5, за исключением волнового сопротивления – 150 Ом. Кабели STP преимущественно используются в сетях Token Ring, но могут применяться и в сетях Fast Ethernet и 100VG-AnyLAN.

4.2.2. Коаксиальный кабель

Коаксиальный кабель состоит из двух концентрических проводников, разделенных слоем диэлектрика. Внешний проводник при этом экранирует внутренний. Такой кабель меньше, чем витая пара, подвержен влиянию внешних электромагнитных помех. Коаксиальный кабель выпускается в нескольких вариантах, различающихся диаметром проводников. Наибольшее применение получил кабель с маркировкой RG-58 (толщина 4,95 мм, диаметр центрального проводника 0,81 мм, волновое сопротивление 50 Ом), так называемый "тонкий" коаксиальный кабель (рис. 4.3). Иногда можно встретить "толстый" (или обычный) коаксиальный кабель с маркировкой RG-8 (толщина ½ дюйма, диаметр центрального проводника 2,17 мм, волновое сопротивление 50 Ом). Сети, использующие коаксиальный кабель, обычно достигают пропускной способности 10 Мбит/с, хотя возможности такого типа кабеля гораздо выше.

Для соединения коаксиальных кабелей используются N-разъемы (“толстый” коаксиал) и BNC-разъемы (“тонкий” коаксиал, рис. 4.4).

Стандарт EIA/TIA-568 описывает требования к коаксиальному кабелю, но в новую редакцию EIA/TIA-568A он не вошел, как устаревший. Коаксиальный кабель, как и витая пара, используется для передачи данных на расстояния до нескольких сотен метров. Стандарт Ethernet ограничивает длину сегмента на “тонком” коаксиальном кабеле до 185м, а на “толстом” – до 500м.

Основное применение коаксиальный кабель нашел в сетях Ethernet. В настоящее время все высокопроизводительные сетевые технологии используют либо витую пару, либо волоконно-оптический кабель и полностью игнорируют коаксиальный кабель.



Рис. 4.3. Коаксиальный кабель



Рис. 4.4. BNC-разъем, T-коннектор и терминатор

4.2.3. Волоконно-оптический кабель

Помимо металлических проводников, при построении сетей используются также и стеклянные (точнее, кварцевые) – волоконно-оптические кабели, передающие данные посредством световых волн. Сердечник такого кабеля представляет собой тонкое кварцевое волокно, заключенное в пластиковую отражающую оболочку. В достаточно тонком волокне (диаметр жилы порядка 5-15 мкм, что сравнимо с длиной световой волны) может распространяться только один световой луч (одна мода). Такой кабель называется **одномодовым** (Single Mode Fiber, SMF). Скорость передачи данных по одномодовому кабелю может

достигать десятков гигабит в секунду. При этом, за счет использования световых волн разной длины, возможна одновременная организация в одном волокне нескольких высокоскоростных каналов. Типичная полоса пропускания одномодового кабеля достигает 900 ГГц.

Однако производство одномодового кабеля довольно сложно, кроме того, для монтажа такого кабеля требуется использование прецизионного оборудования. Поэтому более распространен так называемый **многомодовый** (Multi Mode Fiber, MMF) волоконно-оптический кабель, которому свойственна относительно большая толщина волокна (40-110 мкм). При этом световые лучи, входя в кабель под разными углами, отражаются от стенок волокна, проходят разные расстояния и попадают к приемнику в разное время, искажая друг друга. Существуют способы уменьшения искажений, однако, в основном, за счет уменьшения полосы пропускания. В результате многомодовый волоконно-оптический кабель длиной 100 м может предоставить полосу пропускания в 1600 МГц при длине волны 0.85 мкм.

Передачу сигналов по волокну в настоящее время осуществляют в трех диапазонах: 0.85 мкм, 1.3 мкм и 1.55 мкм. В качестве источника световых волн в волоконно-оптических каналах используют светодиоды (LED, Light Emitting Diode) и лазерные диоды (ILD, Injection Laser Diode). Первое поколение передатчиков (середина 1970-х годов) строилось на основе светодиодов, работающих на длине волны 0.85 мкм в многомодовом режиме. Второе поколение (конец 1970-х) составили одномодовые передатчики, работающие на длине волны 1.3 мкм. В начале 1980-х появились передатчики третьего поколения – лазерные диоды, работающие на длине волны 1.55 мкм. Четвертое поколение оптических передатчиков (начало 1990-х) базируется целиком на лазерных диодах и реализует когерентные системы связи с частотной или фазовой модуляцией сигнала. Пятое поколение базируется на использовании новой технологии легирования световодов, позволяющей значительно усиливать проходящие по световоду сигналы.

Скорость передачи с использованием светодиодов при длине кабеля до 1 км лежит в пределах 10-25 Мбит/с, а с использованием лазерных диодов – в пределах 25-100 Мбит/с. В начале 1990-х годов была создана система связи со скоростью передачи данных в 2.5 Гбит/с на расстояние свыше 2200 км.

Стандарт EIA/TIA-568A определяет два типоразмера многомодового кабеля: 62,5/125 мкм и 50/125 мкм (первое число – диаметр внутреннего проводника, второе – диаметр оболочки).

Волоконно-оптические кабели обладают наилучшими электромагнитными и механическими характеристиками, не подвержены влиянию электромагнитных помех, затрудняют перехват данных, но их монтаж наиболее сложен и трудоемок, требует применения специализированного дорогостоящего оборудования и квалифицированного персонала.

4.3. Беспроводные среды передачи данных

Если по каким-либо причинам соединить компьютеры кабелем не представляется возможным, или сильно затруднено, может оказаться полезным применение беспроводных технологий. Беспроводные сети в основном используют три технологии передачи данных: передача в инфракрасном диапазоне, передача данных с помощью широкополосных радиосигналов и передача данных с помощью обычных (“узкополосных”) радиосигналов.

4.3.1. Инфракрасные волны

Инфракрасные каналы работают в диапазоне высоких частот вплоть до 1000 ГГц, где сигналы мало подвержены влиянию электромагнитных помех, следовательно, передача данных может осуществляться на высокой скорости.

Существует три основных типа инфракрасных каналов: прямой видимости (приемопередатчики направлены друг на друга), рассеянного излучения (волны отражаются от пол, стен, потолка помещения) и отраженного излучения (приемопередатчики направлены на общий отражатель). Основная проблема таких каналов – поглощение и рассеивание инфракрасных волн в атмосфере, сильная зависимость от погодных условий. Даже лист бумаги, случайно оказавшийся между передатчиком и приемником, может полностью блокировать передачу данных.

Использование ненаправленной антенны и маломощного передатчика (100 мВт) ограничивает дальность связи до 30-50 м. Направленная антенна и более мощный передатчик (250 мВт) увеличивают возможную дальность связи до 10 км.

Выпускается оборудование для организации высокоскоростных инфракрасных каналов (до 155 Мбит/с) при дальности связи до 150 м.

4.3.2. Радиоволны, сигналы с узкополосным спектром

Обычный радиосигнал занимает узкую полосу радиоспектра вблизи несущей частоты. Для надежного приема такой сигнал должен обладать значительной энергией. Мощный сигнал, с одной стороны, является сильным источником помех, а с другой – сам сильно подвержен влиянию внешних помех.

В узкополосных системах связи используется полоса частот в диапазоне 18-19 ГГц. Сигнал на этой частоте не может проникать через стены (металлические и бетонные). Для организации компьютерных сетей узкополосные системы практически не применяются.

4.3.3. Радиоволны, широкополосные сигналы

Организация радиоканала, как правило, осуществляется в диапазонах частот около 900 МГц, 2.4 ГГц и 5.7 ГГц. Для работы в этих диапазонах в США

не требуется никакого лицензирования (в России необходимо получить лицензию в Госсвязьнадзоре).

Широкополосный (spread spectrum) сигнал занимает значительно более широкий частотный диапазон, чем тот, что потребовался бы при обычной передаче. Для расширения спектра используются две основные технологии, основанные на использовании псевдослучайного (шумоподобного) кодирования сигнала. Обе технологии лежат в основе стандарта IEEE 802.11.

Первый способ формирования широкополосного сигнала – **метод частотных скачков** (Frequency Hopping Spread Spectrum, FHSS). Весь выделенный диапазон частот разбивается на несколько поддиапазонов (IEEE 802.11 определяет для FHSS разбиение на 79 поддиапазонов). Передатчик постоянно переходит с одного поддиапазона на другой: например, первый бит передается в первом поддиапазоне, второй – в 12, третий – в 7, четвертый – в 53 и т.д. Ясно, что, не зная последовательности и частоты переключения диапазонов, сигнал принять невозможно. Каждая пара приемник – передатчик должна работать на согласованной последовательности поддиапазонов. Кроме того, если в одной полосе одновременно работают несколько передатчиков с разными последовательностями переключения поддиапазонов, то они практически не мешают друг другу. Вероятность случайного совпадения используемых поддиапазонов в некоторый момент времени (и, соответственно, порчи данных) достаточно невелика, так что такие ошибки могут обрабатываться протоколами более высокого уровня.

Второй способ называется **методом прямой последовательности** (Direct Sequence Spread Spectrum, DSSS). При передаче в каждый блок данных встраиваются пустые биты (с псевдослучайными – шумоподобными – значениями). После каждого информационного бита добавляется свое количество пустых битов. Получаемые последовательности битов в DSSS называются чипами. Каждый чип затем передается на своей частоте (IEEE 802.11 определяет для DSSS 11 несущих частот). Восстановление сигнала осуществляется с помощью специального процессора, выделяющего данные из шума с помощью коррелятора.

При использовании миниатюрных ненаправленных антенн возможна передача данных на расстояние до нескольких десятков метров (30-50 м). Максимальная дальность связи при работе со всенаправленной антенной достигает 8 км. Направленные антенны (в условиях прямой видимости) позволяют увеличить дальность связи до 10 км, а с использованием усилителей – до 50 км. Наиболее распространенное в настоящее время оборудование обеспечивает пропускную способность в 2 Мбит/с, хотя встречаются и более высокоскоростные (например, 4 Мбит/с) устройства.

Расширение спектра частот позволяет значительно уменьшить мощность источника сигналов (типичное значение выходной мощности – 30..50 мВт). Радиосигнал с распределенным спектром обладает высокой помехоустойчивостью и надежностью, он способен проникать сквозь здания и другие сооружения, что обеспечивает относительно большую дальность связи (для беспроводных сред). Однако при этом достигается относительно низкая скорость переда-

чи. К недостаткам таких каналов относится и возможная электромагнитная несовместимость отдельных сетей, расположенных недалеко друг от друга.

4.3.4. Спутниковая связь

В зависимости от высоты орбиты, спутники делятся на геостационарные и низкоорбитальные.

Спутники, находящиеся на высоте около 36 тыс. км над экватором, согласно третьему закону Кеплера, имеют период обращения равный 24 часам, и называются **геостационарными** (неподвижными относительно Земли). Применение геостационарных спутников позволяет значительно упростить антенные системы (нет необходимости в приводе, меняющем ориентацию антенны). Четыре геостационарных спутника (расположенные на угловом расстоянии в 90 градусов друг от друга) покрывают всю поверхность Земли. К недостаткам геостационарных спутников относится довольно большая задержка прохождения сигнала (250-300 мс). Кроме того, слишком близко расположенные спутники, работающие в одном диапазоне частот, будут создавать помехи друг для друга. Приемлемое угловое расстояние между такими спутниками составляет 2 градуса, то есть одновременно на геостационарной орбите может находиться не более 180 спутников (работающих в общем диапазоне частот). За счет использования нескольких диапазонов это ограничение несколько смягчается. Традиционно используются частоты (приблизительно) от 3 ГГц до 30 ГГц, что приводит к зависимости качества передачи от погодных условий (дождь, снег).

Спутник связи имеет несколько приемопередатчиков (транспондеров), работающих в разных частотных диапазонах. Количество транспондеров обычно лежит в интервале 12..20, типичная пропускная способность одного транспондера – 50 Мбит/с.

Примеры геостационарных систем – Инмарсат, Runnet. Один из спутников системы Runnet охватывает почти всю территорию России. Диапазоны частот 6.18..6.22 ГГц и 3.855..3.895 ГГц. Диаметр антенны 4,8м.

Низкоорбитальные (высота орбиты – от сотен до единиц тысяч километров) спутники постоянно перемещаются относительно любой точки поверхности Земли. Основной принцип низкоорбитальных систем – большое количество (несколько десятков) спутников, совместно охватывающих весь земной шар. Тогда любая наземная станция может переключаться между спутниками по мере их прохождения.

Самый известный проект низкоорбитальной системы – Иридиум – включает 66 (первоначально планировалось 77) спутников на высоте 750 км. Каждый спутник имеет по 48 лучей по 174 дуплексных канала каждый. Диапазон частот 1610-1626.5 МГц (позволяет использовать питание от аккумуляторов).

Другой проект – Глобалстар – включает 48 спутников на высоте 1400 км, у каждого спутника по шесть сфокусированных лучей по 2800 каналов каждый. Наземная станция в каждый момент времени поддерживает связь с тремя ближайшими спутниками.

4.3.5. Сотовая связь

Сотовая связь основана на применении кабельных и беспроводных каналов на тех участках, где они могут проявить свои сильные стороны. Базовая структура сети создается на основе высокоскоростных кабельных каналов связи, а подключение абонентов производится по радиоканалам, что позволяет обеспечить их мобильность. Хотя основное применение сотовых систем до сих пор лежит в области телефонии, современные сотовые технологии позволяют передавать и произвольные цифровые данные.

Различают три поколения систем сотовой связи:

- аналоговые системы (1-е поколение): AMPS, TACS, NMT 450 и др.;
- цифровые системы (2-е поколение): D-AMPS, GSM, CDMA и др.;
- универсальные цифровые системы (3-е поколение) – пока массово не применяются.

Во всех аналоговых системах для передачи речи применяется частотная модуляция и частотное разделение каналов (полоса, отводимая для одного абонента – от 12.5 до 30 кГц). Недостатки аналоговых систем – малая емкость (недостаточно рациональное использование полосы частот), слабая защита от прослушивания, большие габариты абонентского оборудования. Тем не менее, аналоговый стандарт NMT 450 (“скандинавский стандарт”) является одним из двух Российских федеральных стандартов сотовой связи.

Цифровые системы используют одну из двух разновидностей метода множественного доступа: временное разделение каналов (D-AMPS, GSM) или кодовое разделение каналов (CDMA). Например, в стандарте D-AMPS используется две полосы по 25 МГц, каждая из которых разбита на 832 частотных канала по 30 кГц. Стандарт GSM 900 отводит под один канал полосу в 200 кГц, и в полном диапазоне уместится 124 канала. По каждому каналу передаются кадры, принадлежащие разным абонентам – за счет этого достигается временное разделение. При кодовом разделении используется метод расширения спектра (см. 4.3.3): все абоненты используют общую полосу (около 1 МГц), но данные разных абонентов кодируются разными псевдослучайными последовательностями по методу DSSS.

Системы сотовой связи строятся в виде совокупностей **ячеек** (cell), покрывающих обслуживаемую территорию. Ячейки обычно изображают в виде правильных шестиугольников, соприкасающихся ребрами. Схема сети в этом случае напоминает пчелиные соты, что и послужило причиной возникновения термина “сотовая сеть” (cellular network). В центре каждой ячейки располагается базовая станция (БС), с которой (по радиоканалам) связываются все абоненты, находящиеся в пределах данной ячейки. На базовой станции расположены приемная и передающая антенны (часто используется пара приемных антенн), несколько приемников и передатчиков (работающих на разных поддиапазонах частот из выделенной данной БС полосы частот), контроллер и блок сопряжения с линией связи. Если абонент перемещается в другую ячейку, его начинает обслуживать другая БС. Все БС связаны с центром коммутации, у которого имеется подключение, например, к обычной городской телефонной сети. Если

сеть достаточно крупная, то в ней может присутствовать несколько связанных между собой центров коммутации.

Основным принципом сотовой связи, отличающим ее от других систем связи с мобильными абонентами, является принцип **повторного использования частот** (frequency reuse), позволяющий теоретически неограниченно наращивать емкость системы (реальное ограничение – мощность центра коммутации). Суть его в следующем. В рядом расположенных ячейках используются разные полосы частот, что позволяет соседним БС не конкурировать за общую полосу, а абонентскому оборудованию легко выбирать ближайшую к нему БС (по сигналу максимальной мощности). В то же время, одну и ту же полосу можно использовать в несмежных ячейках. Группу ячеек, в которой каждый частотный диапазон используется только одной ячейкой, называют кластером. В результате, для сети произвольного размера, оказывается достаточным наличие трех непересекающихся частотных диапазонов, то есть сеть может быть разбита на 3-элементные кластеры. Такое разбиение оказывается не очень удобным: хотя ячейки, использующие общую полосу частот, и не соприкасаются, но находятся достаточно близко, чтобы создавать друг другу помехи. Поэтому чаще используют кластеры с большим количеством элементов.

5. ПЕРЕДАЧА ДАННЫХ И КОДИРОВАНИЕ ИНФОРМАЦИИ

Сутью передачи данных по некоторому каналу является воспроизведение получателем некоторой (заданной отправителем) функции, например, изменения тока или напряжения во времени. При распространении сигнала происходит его искажение: затухание, искажение формы, смешивание с шумом и пр. Затухание возникает из-за того, что часть энергии сигнала рассеивается, при этом, чем больше длина канала, тем больше затухание. Кроме того, сигналы разных частот затухают не одинаково. Искажение формы сигнала происходит по причине разной скорости распространения сигналов разной частоты. В результате гармоника соседних сигналов могут смешиваться и искажать друг друга. Причиной шума является наличие других источников энергии (кроме передатчика). Источником шума могут быть, например, другие линии передачи данных, силовые электрические кабели, атмосферные явления. Неизбежной разновидностью шума является тепловой шум (при температуре среды больше абсолютного нуля).

5.1. Количество информации и энтропия

Источник информации, который может в каждый момент времени находиться в одном из возможных состояний, называется дискретным источником информации. Будем называть конечное множество всех возможных состояний $\{u_1, u_2, \dots, u_N\}$ **алфавитом** источника (N – размер алфавита или число возможных состояний). В общем случае разные состояния u_i выбираются источником с разной вероятностью p_i , и его можно охарактеризовать совокупностью алфави-

та и множества вероятностей состояний – **ансамблем** $U_N = \{u_1, p_1, u_2, p_2, \dots, u_N, p_N\}$. Разумеется, сумма вероятностей всех состояний должна быть равна 1.

Введем меру неопределенности состояния источника $H(U)$, удовлетворяющую следующим условиям:

- монотонность: мера должна монотонно возрастать с ростом количества возможных состояний.
- аддитивность: мера, вычисленная для сложного источника, состоящего из двух независимых источников (с размерами алфавитов N и M , тогда размер алфавита сложного источника — NM), должна равняться сумме мер этих двух источников. Согласно условию аддитивности, мера должна удовлетворять соотношению $H(U_{NM}) = H(U_M) + H(U_N)$.

Кроме того, существует граничное условие: мера неопределенности для источника с размером алфавита 1 должна равняться 0.

Можно показать, что этим условиям удовлетворяет логарифмическая функция (с произвольным основанием).

Для источника с алфавитом размера N и равновероятными состояниями ($p_i = 1/N$ для любого i) логарифмическая мера была предложена Р.Хартли в 1928 году и имеет вид: $H(U_N) = \log(N)$. Предположение о равновероятности состояний источника информации называется моделью Хартли. Если основание логарифма выбрать равным двум, соответствующая единица неопределенности будет соответствовать неопределенности выбора из двух равновероятных событий и называться **двоичной единицей** или **битом** (от англ. bit, сокращенного binary digit – двоичная единица).

Модели Хартли недостает учета вероятностей состояний. Если, например, источник имеет два возможных состояния с вероятностями 0.999 и 0.001. Ясно, что мера неопределенности такого источника должна быть меньше 1 бита: есть большая уверенность в выборе первого состояния. Если вероятности состояний отличаются незначительно (например, 0.51 и 0.49), то и мера неопределенности должна измениться незначительно по сравнению с равновероятным случаем.

Таким образом, мера неопределенности должна зависеть от вероятностей состояний источника, от всего ансамбля. Такая модель источника информации называется моделью Шеннона. Мера неопределенности выбора дискретным источником состояния из ансамбля U_N называется **энтропией дискретного источника информации** или **энтропией конечного ансамбля**:

$$H(U_N) = -C \sum_{i=1}^N p_i \log p_i$$

где C – произвольное положительное число.

При равновероятности состояний источника мера Шеннона сводится к мере Хартли.

Доказано, что приведенная функция – единственная, удовлетворяющая всем перечисленным условиям.

Термин “энтропия” был заимствован из термодинамики и использован для меры неопределенности из-за того, что обе энтропии – термодинамическая

и информационная – характеризуют степень разнообразия состояний рассматриваемой системы и описываются аналогичными функциями.

5.2. Свойства энтропии

1. Энтропия является неотрицательной вещественной величиной. Это так, поскольку вероятность лежит в интервале от 0 до 1, ее логарифм отрицателен, а значение $-p_i \log p_i$ положительно.
2. Энтропия ограничена сверху значением 1.
3. Энтропия равна 0, только если одно из состояний имеет вероятность, равную 1 (полностью определенный источник).
4. Энтропия максимальна, когда все состояния источника равновероятны. При этом $H_{\max}(U_N) = \log_2 N$.
5. Энтропия источника с двумя состояниями изменяется от 0 до 1, достигая максимума при равенстве их вероятностей.
6. Энтропия объединения нескольких независимых источников информации равна сумме энтропий исходных источников.
7. Энтропия характеризует среднюю неопределенность выбора одного состояния из ансамбля, не учитывая содержательную сторону (семантику) состояний.
8. Энтропия как мера неопределенности согласуется с экспериментальными психологическими данными. Время безошибочной реакции на последовательность случайно чередующихся равновероятных раздражителей растет с увеличением их числа так же, как энтропия, а при переходе к неравновероятным раздражителям, среднее время реакции снижается так же, как энтропия.

5.3. Единицы количества информации

Бит – очень мелкая единица измерения количества информации. Более крупная единица – байт, состоящий из восьми битов. (Восьмибитный байт стал стандартным только с распространением системы IBM System 360 (ЕС ЭВМ), до того в разных вычислительных системах использовались байты разного размера.)

Применяются и более крупные единицы:

Килобайт (Кбайт) – 1024 байт – 2^{10} байт

Мегабайт (Мбайт) – 1024 Кбайт – 2^{20} байт

Гигабайт (Гбайт) – 1024 Мбайт – 2^{30} байт

Терабайт (Тбайт) – 1024 Гбайт – 2^{40} байт

Петабайт (Пбайт) – 1024 Тбайт – 2^{50} байт

В качестве единицы количества информации можно было бы выбрать количество информации, содержащееся, например, в выборе одного из десяти равновероятных сообщений. Такая единица будет называться **дит** или **десятичной единицей**.

5.4. Качество обслуживания

Качество обслуживания (Quality of Service, QoS) сетью потребителя ее услуг определяется, в основном, производительностью и надежностью. Производительность характеризуется следующими основными параметрами:

- Время реакции сети – интегральная характеристика сети с точки зрения пользователя – интервал времени между возникновением запроса пользователя к сетевой службе и получением ответа на этот запрос.
- Пропускная способность или скорость передачи данных – объем данных, переданных за единицу времени. Пропускная способность может, измеряться в битах в секунду (бит/с) или в пакетах в секунду. Различают среднюю, мгновенную и максимальную пропускную способность.
- Задержка доставки данных – время от передачи блока информации до его приема. Часто задержку передачи (вносимую каким-либо сетевым устройством) определяют как интервал времени между моментом поступления пакета на вход сетевого устройства и моментом появления его на выходе этого устройства. Обычно качество сети характеризуется максимальной задержкой передачи и вариацией задержки.

Надежность оценивается, среди прочих, следующими характеристиками:

- Коэффициент готовности – доля времени, в течение которого система может быть использована.
- Уровень ошибок – определяется как вероятность безошибочной передачи определенного объема данных. Например, вероятности 0,99999 соответствует 1 ошибочный бит на 100000 переданных битов. Для локальных сетей характерен уровень ошибок 1 на 10^8 - 10^{12} бит.

Максимальная скорость передачи для канала без шума (идеальный случай), согласно теореме Найквиста, составляет $2N\log_2 V$, где N – пропускная способность, V – количество различаемых уровней сигнала.

Для реальных каналов (с шумом) максимальная скорость передачи определяется по теореме Шеннона: $N\log_2(1+S/N)$, где S/N – отношение мощности полезного сигнала к мощности шума (“отношение сигнал-шум”).

5.5. Кодирование информации

При передаче цифровой информации с помощью цифровых сигналов применяется цифровое кодирование, управляющее последовательностью прямоугольных импульсов в соответствии с последовательностью передаваемых данных. При цифровом кодировании применяют либо потенциальные, либо импульсные коды. При **потенциальном кодировании** информативным является уровень сигнала. При **импульсном кодировании** используются либо перепады уровня (транзитивное кодирование), либо полярность отдельных импульсов (униполярное, полярное, биполярное кодирование). В отдельную группу импульсных кодов выделяют двухфазные коды, при которых в каждом битовом интервале обязательно присутствует переход из одного состояния в другое (та-

кие коды позволяют выделять синхросигнал из последовательности состояний линии, то есть являются самосинхронизирующимися).

Наиболее распространены следующие коды:

- NRZ (Non-Return to Zero – без возврата к нулю) – потенциальный код, состояние которого прямо или инверсно отражает значение бита данных
- дифференциальный NRZ – состояние меняется в начале битового интервала для “1” и не меняется при “0”
- NRZI (Non-Return to Zero Inverted – без возврата к нулю с инверсией) – состояние меняется в начале битового интервала при передаче “0” и не меняется при передаче “1”. Используется в FDDI, 100BaseFX.
- RZ (Return to Zero – с возвратом к нулю) – биполярный импульсный самосинхронизирующийся код, представляющий “1” и “0” импульсами противоположной полярности, длящимися половину такта (вторую половину такта состояния устанавливается в нулевое); всего используется три состояния
- AMI (Bipolar Alternate Mark Inversion – биполярное кодирование с альтернативной инверсией) – используется три состояния: 0, + и –, для кодирования логического нуля используется состояние 0, а логическая единица кодируется по очереди состояниями + и –. Используется в ISDN, DSx.
- Манчестерское кодирование (manchester encoding) – двухфазное полярное самосинхронизирующееся кодирование, логическая единица кодируется перепадом потенциала в середине такта от низкого уровня к высокому, логический ноль – обратным перепадом (если необходимо представить два одинаковых значения подряд, в начале такта происходит дополнительный служебный перепад потенциала). Используется в Ethernet.
- Дифференциальное манчестерское кодирование (differential manchester encoding) – двухфазное полярное самосинхронизирующееся кодирование, логический ноль кодируется наличием перепада потенциала в начале такта, а логическая единица – отсутствием перепада; в середине такта перепад есть всегда (для синхронизации). В Token Ring применяется модификация этого метода, кроме “0” и “1”, использующая служебные биты “J” и “K”, не имеющие перепада в середине такта (“J” не имеет перепада в начале такта, “K” – имеет).
- MLT-3 – трехуровневое кодирование со скремблированием без самосинхронизации, логический ноль кодируется сохранением состояния, а логическая единица кодируется по очереди следующими состояниями: +V, 0, -V, 0, +V и т.д. Используется в FDDI и 100BaseTX.
- PAM5 (Pulse Amplitude Modulation) – пятиуровневое биполярное кодирование, при котором каждая пара бит данных представляется одним из пяти уровней потенциала. Применяется в 1000BaseT.
- 2B1Q (2 Binary 1 Quarternary) – пара бит данных представляется одним четвертичным символом, т.е. одним из четырех уровней потенциала. Применяется в ISDN.

0	1	0	1	1	0	0	0	1
---	---	---	---	---	---	---	---	---

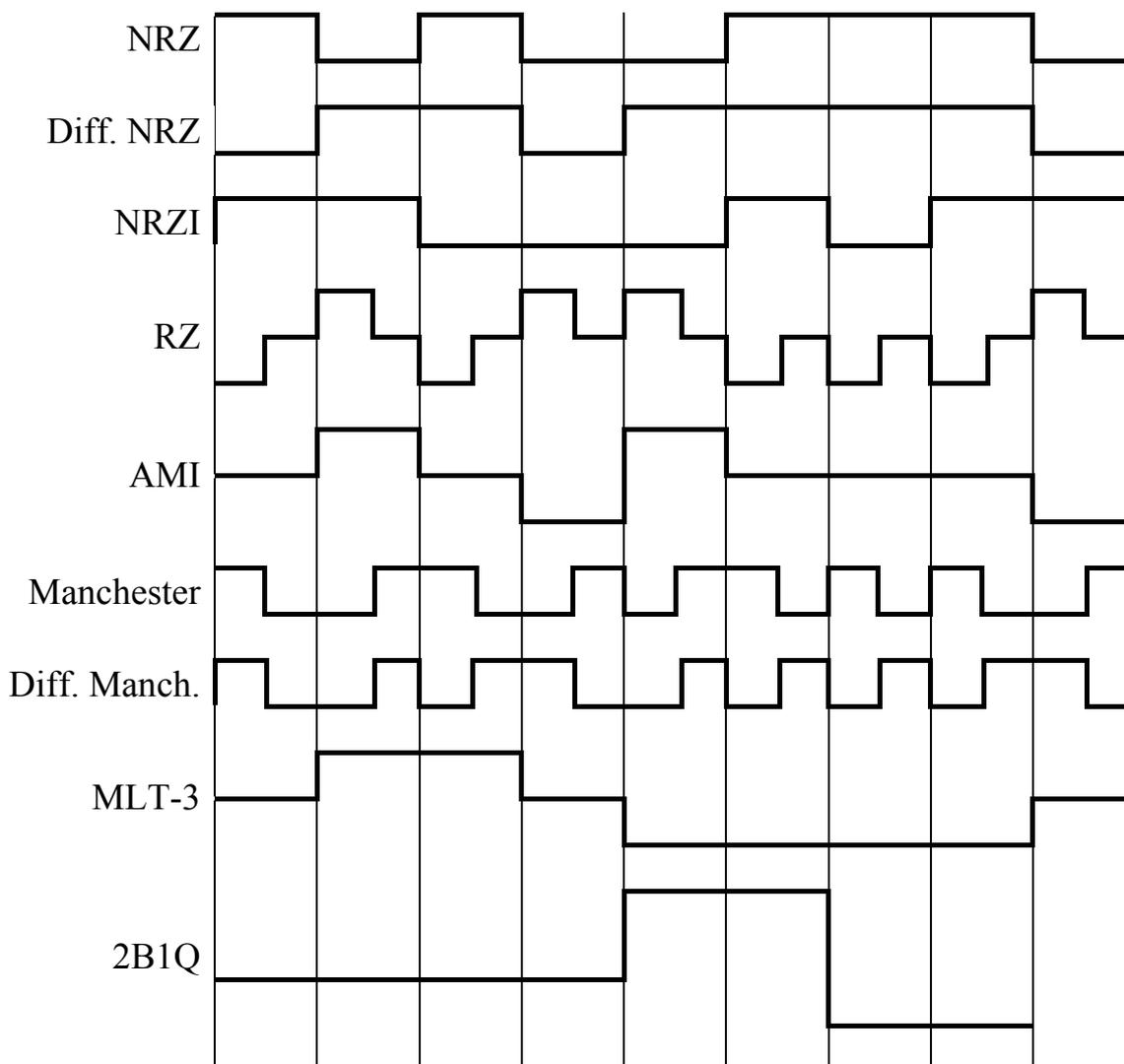


Рис.5.1. Способы цифрового кодирования данных

5.6. Логическое кодирование

Некоторые разновидности цифрового кодирования очень чувствительны к характеру передаваемых данных. Например, при передаче длинных последовательностей логических нулей посредством потенциального кода типа NRZ или AMI сигнал на линии долгое время не изменяется, и приемник может ошибиться с моментом считывания очередного бита. Для кода NRZ подобные проблемы возникают и при передаче длинных последовательностей логических единиц. Логическое кодирование (которому может подвергаться исходная последовательность данных) должно внедрять в длинные последовательности бит, биты с противоположным значением, или вообще заменять их другими последовательностями. Кроме исключения “проблемных” битовых последовательностей, логическое кодирование позволяет также увеличить кодовое расстояние между символами (для упрощения декодирования), улучшить спектральные характеристики сигнала, а кроме того передавать в общем потоке служебные сигналы. В основном для логического кодирования применяются три группы методов: вставка бит, избыточное кодирование и скремблирование.

Вставка бит (bit stuffing) – наиболее прямолинейный способ исключения длинных последовательностей, например, логических единиц. Если в передаваемой последовательности встречается непрерывная цепочка “1”, то передатчик вставляет “0” после каждой, например, пятой “1”. Приемник отбрасывает все эти лишние “0”, которые встречаются после пяти “1”. Разумеется, можно проводить и обратную операцию – вставку “1” в длинные последовательности “0”. Схема вставки бит применяется, например, в протоколе HDLC.

Избыточное кодирование основано на разбиении исходной последовательности бит на участки одинаковой длины – символы. Затем каждый символ заменяется (как правило, табличным способом) на новый, имеющий либо большее количество бит, либо другое основание системы счисления (например, на символ, состоящий из троичных разрядов). Рассмотрим некоторые распространенные схемы логического кодирования.

Логический код 4В/5В заменяет каждые 4 бита входного потока (исходный символ) на 5-битный выходной символ. Так как количество различных 5-битных символов равно 32, а исходные символы могут содержать лишь одну из 16 битовых комбинаций, среди возможных выходных кодов можно отобрать 16 “удобных” комбинаций – не содержащих большого количества нулей (больше трех подряд), среди оставшихся кодов выделить служебные символы (для поддержания синхронизации, выделения границ кадров и их полей и т.д.), а оставшиеся коды считать запрещенными.

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

Табл. 5.1. Код 4В/5В

Накладные расходы при кодировании 4В/5В составляют 25% (один лишний бит на четыре бита данных), соответственно для достижения той же пропускной способности, что и без логического кодирования, передатчик должен работать на повышенной на 25% частоте. Код 4В/5В используется в FDDI и Fast Ethernet: 100BaseFX и 100BaseTX.

Логический код 8В/10В заменяет каждый 8-битный исходный символ 10-битным выходным символом. При том же уровне накладных расходов (25%), что в случае кода 4В/5В, обладает 4-кратной избыточностью (1024 выходных символов и 256 исходных символов). При кодировании 8В/10В каждому исходному символу сопоставлено два выходных символа, выбор из которых осуще-

ствляется в зависимости от последнего бита предыдущего переданного символа. В результате код обеспечивает стабильное соотношение “0” и “1” в выходном потоке, независимо от исходных данных. Это свойство важно для лазерных передатчиков, поскольку от данного соотношения зависит их нагрев и количество ошибок приема. Код 8В/10В используется в Gigabit Ethernet: 1000BaseSX, 1000BaseLX, 1000BaseCX.

Логический код 8В/6Т кодирует каждые 8 бит исходной информации шестью троичными (Т – ternary, троичный) разрядами, принимающими значения $\{+, 0, -\}$. Например, “00000000” = “+–00+–”, “11111110” = “–+0+00”. Избыточность кода 8В/6Т выше, чем у кода 4В/5В и составляет $3^6/2^8 = 729/256 = 2,85$. Применяется в Fast Ethernet – 100BaseТ4.

Скремблирование заключается в побитном вычислении выходной последовательности на основании значений бит исходной последовательности и уже вычисленных бит результата. Например, скремблер может вычислять для каждого бита следующее выражение: $V_i = A_i \oplus V_{i-5} \oplus V_{i-7}$, где A_i – i -й бит исходной последовательности, V_i – i -й бит результата скремблирования, \oplus – операция сложения по модулю два. Различные алгоритмы скремблирования отличаются разным количеством слагаемых и разным сдвигом между слагаемыми (в приведенном выше примере используется два слагаемых со сдвигами 5 и 7). Например, в ISDN используется два варианта скремблирования: со сдвигами 5 и 23, и со сдвигами 18 и 23.

Существуют специальные методы скремблирования, применяемые совместно определенными методами физического кодирования. Например, для улучшения кода АМІ применяются методы В8ZS и HDB3. Метод В8ZS (Bipolar with 8-Zeros Substitution, биполярный с заменой 8 нулей) заменяет последовательности, состоящие из 8 нулей на “000V10V1”, где V – сигнал единицы запрещенной в данном такте полярности, а 1 – сигнал единицы корректной полярности. Если на 8 тактах приемник наблюдает три начальных нуля и два искажения полярности, то он заменяет эти 8 бит на 8 логических нулей. Метод HDB3 (High-Density Bipolar 3-Zeros, биполярный трех-нулевой высокой плотности) заменяет последовательности из четырех идущих подряд нулей на один из четырех четырехразрядных биполярных кодов в зависимости от предыстории – полярности предыдущего импульса и предыдущей замены.

5.7. Самосинхронизирующиеся коды

Коды, позволяющие выделять синхросигнал из последовательности состояний линии, называются самосинхронизирующимися. При использовании таких кодов отпадает необходимость в отдельной синхронизации передатчика и приемника.

Одна из возможных реализаций самосинхронизирующих кодов – двух-фазные коды, в каждом битовом интервале которых обязательно присутствует переход из одного состояния в другое.

Большинство технологий локальных сетей используют именно самосинхронизирующие коды: в Ethernet применяется манчестерский код, в Token Ring – вариант дифференциального манчестерского кода

6. КОНТРОЛЬ ПЕРЕДАЧИ ИНФОРМАЦИИ И СЖАТИЕ ДАННЫХ

6.1. Самовосстанавливающиеся коды

Одним из средств борьбы с помехами являются **самовосстанавливающиеся** (корректирующие) коды, позволяющие не только обнаружить, но и исправить ошибки при приеме.

Пусть используется n -разрядный двоичный код. Ошибка при приеме кодовой комбинации состоит в том, что (под влиянием помехи) либо переданный нуль был принят, как единица, либо единица была принята, как нуль. Если в кодовой комбинации ошибка присутствует только в одном разряде, то такую ошибку будем называть одиночной, если в двух разрядах – двойной и т.д.

Если при передаче в качестве информационных используются все возможные кодовые комбинации, ошибки невозможно даже обнаружить: любая ошибка преобразует кодовую комбинацию в другую допустимую кодовую комбинацию. Для распознавания ошибок необходимо часть кодовых комбинаций зарезервировать для контроля ошибок. Для того, чтобы было можно обнаружить одиночную ошибку, достаточно в качестве информационных взять такие кодовые комбинации, которые различались бы между собой не менее, чем в двух знаках. Тогда одиночная ошибка в любой информационной кодовой комбинации приводила бы к появлению запрещенной кодовой комбинации. Для исправления одиночных ошибок, можно использовать код, информационные кодовые комбинации которого различаются не менее, чем в трех знаках. Тогда одиночная ошибка даст запрещенную кодовую комбинацию, отличающуюся от исходной в одном знаке, но отличающуюся от любой другой разрешенной комбинации не менее, чем в двух знаках. Соответственно, можно будет не только обнаружить ошибку, но и найти истинную передававшуюся кодовую комбинацию.

Аналогичным образом можно построить коды, обнаруживающие и исправляющие ошибки любой кратности. Для этого нужно лишь уменьшать долю информационных кодовых комбинаций среди всех возможных.

При таком подходе необходимо каждую принятую кодовую комбинацию сравнивать со всеми разрешенными комбинациями и, в случае совпадения, считать, что ошибки не было, а в противном случае считать истинной разрешенную комбинацию, отличающуюся от принятой в минимальном количестве разрядов. Это – довольно малоэффективный метод обнаружения и исправления ошибок.

6.2. Систематические коды

Другой подход к построению кодов – разделение разрядов кода на информационные и контрольные. Такие коды называются систематическими. Пусть всего в коде n разрядов, из них k – информационных и r – контрольных разрядов ($n=k+r$). Такой код может передавать $N = 2^k$ различных сообщений. Из r контрольных разрядов можно организовать 2^r различных комбинаций. Для обнаружения и исправления одиночной ошибки нужно, во-первых, указать наличие/отсутствие ошибки и, во-вторых, указать номер разряда, в котором произошла ошибка.

Таким образом, чтобы в контрольных разрядах можно было передавать информацию для исправления одиночных ошибок, их количество должно удовлетворять неравенству $2^r \geq n+1$ или $2^n/(n+1) \geq N$. Если достигается равенство: $2^n/(n+1) = N$, то количество контрольных разрядов, приходящихся на один информационный, будет наименьшим. Например, для $N=4$ различных сообщений ($k=2$) наименьшее значение n равно пяти ($2^4/(4+1) = 3,2 < 4$, а $2^5/6 \approx 5,3 > 4$). Значит, количество контрольных разрядов, необходимое для обнаружения и исправления одиночных ошибок $r = n-k = 5-2 = 3$.

6.3. Алгоритмы сжатия данных

В общем смысле под сжатием данных понимают такое их преобразование, что его результат занимает меньший объем памяти. При этом (по сравнению с исходным представлением) экономится память для их хранения и сокращается время передачи сжатых данных по каналам связи. Синонимы термина “сжатие” – упаковка, компрессия, архивация. Обратный процесс (получение исходных данных по сжатым) называется распаковкой, декомпрессией, восстановлением.

Качество сжатия характеризуется коэффициентом сжатия, равным отношению объема сжатых данных к объему исходных данных.

В зависимости от возможной точности восстановления исходных данных, различают сжатие без потерь (данные восстанавливаются точно в исходном виде) и сжатие с потерями (восстановленные данные не идентичны исходным, но их различиями в том контексте, в котором эти данные используются, можно пренебречь). Сжатие с потерями применяется, например, для упаковки многоцветных фотографических изображений (алгоритм JPEG), звука (алгоритм MP3), видео (группа алгоритмов MPEG). При этом используются особенности человеческого восприятия: например, глаз человека не может различить два

близких оттенка цвета, закодированных 24 битами, поэтому можно без видимых искажений уменьшить разрядность представления цвета.

Для многих разновидностей данных – текстов, исполняемых файлов и т.д. – допустимо применение только алгоритмов сжатия без потерь.

Сжатие без потерь, в основном, базируется на двух группах методов: словарных и статистических. Словарные методы используют наличие повторяемых групп данных и, например, записывают первое вхождение повторяемого участка непосредственно, а все последующие вхождения заменяют на ссылку на первое вхождение. Другие словарные методы отдельно хранят словарь в явной форме и заменяют все вхождения словарных терминов на их номер в словаре.

Статистические методы используют тот факт, что частота появления в данных различных байтов (или групп байтов) неодинакова, следовательно, часто встречающиеся байты можно закодировать более короткой битовой последовательностью, а редко встречающиеся – более длинной. Часто в одном алгоритме используют и словарные, и статистические методы.

6.3.1. Алгоритм RLE

Самый простой из словарных методов – RLE (Run Length Encoding, кодирование переменной длины) умеет сжимать данные, в которых есть последовательности повторяющихся байтов. Упакованные RLE данные состоят из управляющих байтов, за которыми следуют байты данных. Если старший бит управляющего байта равен 0, то следующие байты (в количестве, записанном в семи младших битах управляющего байта) при упаковке не изменялись. Если старший бит равен 1, то следующий байт нужно повторить столько раз, какое число записано в остальных разрядах управляющего байта.

Например, исходная последовательность

00000000 00000000 00000000 00000000 11001100 10111111 10111011

будет закодирована в следующем виде (выделены управляющие байты):

10000100 00000000 **00000011** 11001100 10111111 10111011.

А, например, данные, состоящие из сорока нулевых байтов, будут закодированы всего двумя байтами: **1010 1000** 00000000.

6.3.2. Алгоритм Лемпела-Зива

Наиболее широко используются словарные алгоритмы из семейства LZ, чья идея была описана Лемпелом и Зивом в 1977 году. Существует множество модификаций этого алгоритма, отличающихся способами хранения словаря, добавления слова в словарь и поиска слова в словаре.

Словом в этом алгоритме называется последовательность символов (не обязательно совпадающая со словом естественного языка). Слова хранятся в словаре, а их вхождения в исходные данные заменяются адресами (номерами) слов в словаре. Некоторые разновидности алгоритма хранят отдельно словарь и отдельно упакованные данные в виде последовательности номеров слов. Другие считают словарем весь уже накопленный результат сжатия. Например, сжа-

тый файл может состоять из записей вида $[a,l,t]$, где a – адрес (номер позиции), с которой начинается такая же строка длины l , что и текущая строка. Если $a > 0$, то запись считается ссылкой на словарь и поле t (текст) в ней – пустое. Если $a = 0$, то в поле t записаны l символов, которые до сих пор в такой последовательности не встречались.

Алгоритм сжатия заключается в постоянном поиске в уже упакованной части данных максимальной последовательности символов, совпадающей с последовательностью, начинающейся с текущей позиции. Если такая последовательность (длины > 3) найдена, в результат записывается ее адрес и длина. Иначе в результат записывается 0, длина последовательности и сама (несжатая) последовательность.

6.3.3. Кодирование Шеннона-Фано

Методы эффективного кодирования сообщений для передачи по дискретному каналу без помех, предложенные Шенноном и Фано, заложили основу статистических методов сжатия данных. Код Шеннона-Фано строится следующим образом: символы алфавита выписывают в таблицу в порядке убывания вероятностей. Затем их разделяют на две группы так, чтобы суммы вероятностей в каждой из групп были максимально близки (по возможности, равны). В кодах всех символов верхней группы первый бит устанавливается равным 0, в нижней группы – 1. Затем каждую из групп разбивают на две подгруппы с одинаковыми суммами вероятностей, и процесс назначения битов кода продолжается по аналогии с первым шагом. Кодирование завершается, когда в каждой группе останется по одному символу.

Качество кодирования по Шеннону-Фано сильно зависит от выбора разбиений на подгруппы: чем больше разность сумм вероятностей подгрупп, тем более избыточным оказывается код. Для дальнейшего уменьшения избыточности, используют кодирование крупными блоками – в качестве “символов” используются комбинации исходных символов сообщения, но и этот подход имеет те же ограничения. От указанного недостатка свободна методика кодирования Хаффмана.

6.3.4. Алгоритм Хаффмана

Алгоритм Хаффмана гарантирует однозначное построение кода с наименьшим для данного распределения вероятностей средним числом символов кода на символ сообщения. На первом шаге подсчитываются частоты всех символов в исходных данных. На втором шаге строятся новые коды (битовые последовательности) для каждого символа, так, чтобы никакие две разные последовательности не имели общего начала, например, три последовательности 0, 10, 110. удовлетворяют этому требованию. Хаффман предложил строить двоичное дерево символов, в корне которого находится наиболее частый символ, на расстоянии 1 от корня – следующие по частоте символы, и так далее. На основе такого дерева коды для символов получаются путем выполнения простой

процедуры обхода дерева. Код представляет собой путь от корня до символа, в котором 1 означает переход по левой ветви, а 0 – по правой. Такой способ построения гарантирует нужное свойство кодов. Наконец, на последнем шаге в выходные данные записывается построенное дерево, а за ним следуют закодированные данные.

Алгоритм Хаффмана обеспечивает высокую скорость упаковки и распаковки, но степень сжатия, достигаемая при его использовании, довольно невелика. Одним из недостатков этого алгоритма является необходимость двух проходов по данным – на первом проходе подсчитываются частоты, строится дерево и формируются коды, а на втором выполняется собственно кодирование. Этому недостатка лишен адаптивный алгоритм Хаффмана, пересчитывающий частоты символов (и, соответственно, изменяющий коды) по мере поступления данных.

7. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ЛОКАЛЬНЫХ СЕТЕЙ

Локальные сети расположены на небольшой площади – комната, здание, несколько соседних зданий. Максимальное расстояние между компьютерами – несколько сотен метров. Количество компьютеров невелико – несколько десятков, максимум единицы сотен.

Расположение в одном здании позволяет применять кабели (а не более дорогие беспроводные технологии). Небольшие расстояния позволяют достигать приемлемых скоростей передачи даже по дешевым кабелям (или больших скоростей, но по более дорогим кабелям). Малое количество компьютеров допускает использование общей разделяемой среды передачи, в том числе в режиме разделения времени.

В ЛВС в качестве кабельных сред передачи используются коаксиальный кабель, витая пара и оптоволоконный кабель. Для ЛВС характерно использование следующего сетевого оборудования:

- приемопередатчики (transceiver)
- повторители (repeater) – для объединения коаксиальных сегментов
- концентраторы (hub) – для формирования звезд и деревьев на витой паре
- мосты (bridge) – для объединения локальных сетей (возможно, с разными технологиями) и изоляции внутреннего трафика подсетей
- коммутаторы (switch) – для высокоскоростного одновременного соединения нескольких пар абонентов
- маршрутизаторы (router) – для управления путями передачи данных в сегментированных сетях.

7.1. Сетевые топологии

Понятие "топология" описывает структуру, образуемую узлами сети и каналами связи, то есть свойства сетей, не зависящие от размера сети.

Для сетей с селекцией данных характерны ширококвещательные топологии. Их основные разновидности – шина, дерево, звезда с пассивным центром.

Для сетей с маршрутизацией данных характерны последовательные ("точка-точка") топологии: звезда с интеллектуальным центром, кольцо, цепочка, полносвязная, произвольная.

7.1.1. Шина

Для организации сети минимально необходима одна линия передачи данных и по одному сетевому интерфейсу для каждого участника сети. Такая топология называется шинной (другое название – моноканал). К единственной незамкнутой линии передачи данных в произвольных точках подключаются все участники.

Шина позволяет легко добавлять новых участников к сети, для прокладки линии требуется минимальное количество кабеля. Основной недостаток – любой разрыв линии делает сеть неработоспособной.

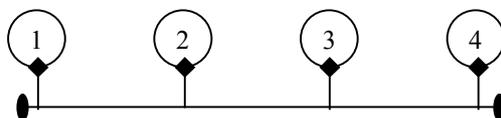


Рис.7.1. Топология "шина"

7.1.2. Дерево

Если несколько шин – сегментов соединить с помощью концентраторов или повторителей, то разрыв в одном сегменте делает неработоспособным только этот сегмент, а все остальные сегменты продолжают функционировать. Такая топология носит название "дерево".

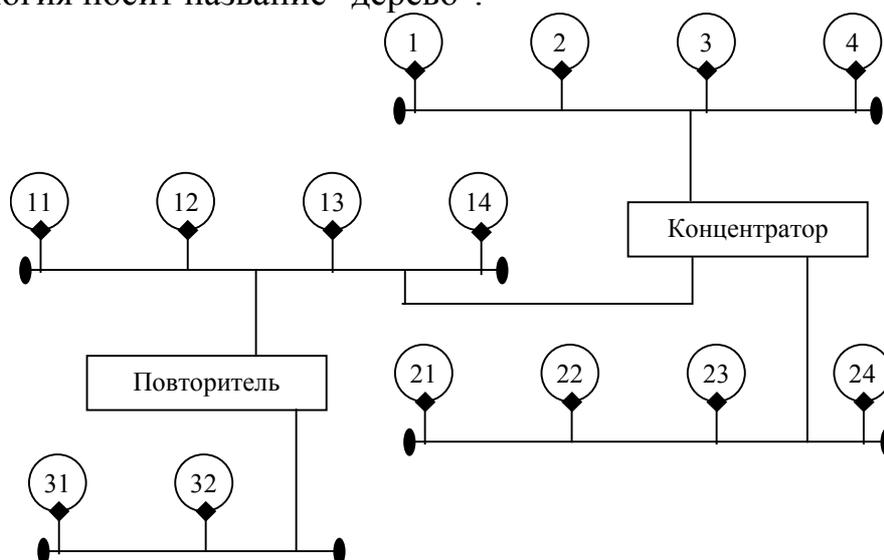


Рис.7.2. Топология "дерево"

7.1.3. Звезда с пассивным центром

Звездообразная топология требует наличия специального многопортового устройства – концентратора. Концентратор соединяется с каждым участником сети отдельной линией передачи данных. При выходе из строя одной из линий доступ к сети теряет только один участник. Однако, если откажет коммутатор, работа сети станет полностью невозможной.

Как правило, концентраторы являются пассивным оборудованием, просто передающим пришедшие по одной из линий данные во все остальные линии.

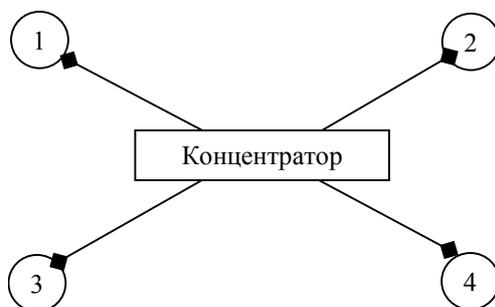


Рис.7.3. Топология “звезда”

7.1.4. Звезда с интеллектуальным центром

Если в предыдущей топологии заменить пассивный концентратор на активное оборудование - интеллектуальный концентратор, коммутатор или маршрутизатор, то появится возможность отказаться от неэффективной передачи данных по всем линиям, когда получатель подключен только к одной из них. Активное оборудование обладает информацией о структуре сети и может выбирать путь передачи данных, передавая данные только тому участнику, для которого они предназначены и не загружая остальные линии.

7.1.5. Кольцо

При кольцеобразной топологии каждый участник соединен отдельной линией передачи данных с двумя соседями. Данные по каждой линии передаются обычно только в одном направлении. Блоки данных ретранслируются каждым очередным участником до тех пор, пока не попадут к получателю. Как правило, после этого блок продолжают передавать по кольцу дальше. Отправитель, получив свой блок, прошедший полный круг, изымает его из кольца и удаляет. Основной недостаток кольцевой топологии – при обрыве хотя бы одной линия, или выходе из строя хотя бы одного участника, сеть перестает функционировать.



Рис.7.4. Топология “кольцо”

7.1.6. Цепочка

Эта топология получается из кольца при удалении одной из линий. В отличие от кольца, линии должны передавать данные в обоих направлениях.

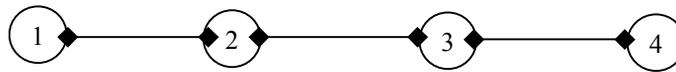


Рис.7.5. Топология “цепочка”

7.1.7. Полносвязная топология

Предельный максимальный случай, полностью связная сеть "каждый с каждым", при n участниках требует наличия $n*(n-1)/2$ ЛПД и $n*(n-1)$ сетевых интерфейсов. Например, полностью связная сеть, соединяющая 4 компьютера ($n=4$) состоит из $4*3/2=6$ ЛПД и $4*3=12$ сетевых интерфейсов (см. рис).

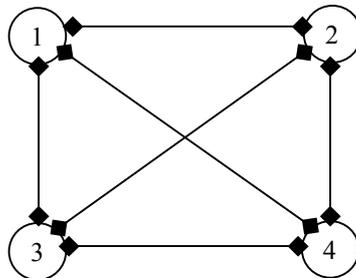


Рис.7.6. Полносвязная топология

Выход из строя любой одной линии передачи данных (возможно, даже нескольких линий) не влияет на работу сети – можно найти другой маршрут для передачи данных. Недостаток – наибольшее среди всех топологий требуемое количество оборудования и кабелей.

7.1.8. Произвольная (ячеистая) топология

Топология, получаемая из полностью связной удалением одной или нескольких линий. Единственное ограничение – полученная сеть должна быть связной.

Такая топология позволяет обеспечить высокую надежность связи (за счет нескольких возможных путей передачи данных) там, где это нужно, не расходуя излишние средства на оборудование и кабель там, где этого не требуется.

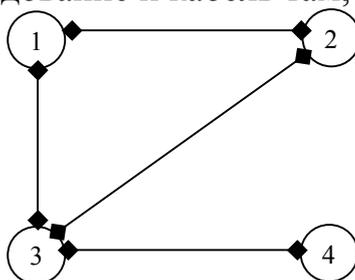


Рис.7.7. Ячеистая топология

7.2. Методы доступа и их классификация

Метод доступа (access method) – это набор правил, регламентирующих способ получения в пользование (“захвата”) среды передачи. Метод доступа определяет, каким образом узлы получают возможность передавать данные.

Выделяют следующие классы методов доступа:

- селективные методы,
- состязательные методы (методы случайного доступа),
- методы, основанные на резервировании времени,
- кольцевые методы.

Все методы доступа, кроме состязательных, образуют группу методов детерминированного доступа.

При использовании селективных методов для того, чтобы узел мог передавать данные, она должна получить разрешение. Метод называется **опросом** (polling), если разрешения передаются всем узлам по очереди специальным сетевым оборудованием. Метод называется **передачей маркера** (token passing), если каждая узел по завершении передачи передает разрешение следующей.

Методы **случайного доступа** (random access methods) основаны на “состязании” узлов за получение доступа к среде передачи. Случайный доступ может быть реализован различными способами: базовым асинхронным, с тактовой синхронизацией моментов передачи кадров, с прослушиванием канала перед началом передачи (“слушай, прежде чем говорить”), с прослушиванием канала во время передачи (“слушай, пока говоришь”). Могут быть использованы одновременно несколько способов из перечисленных.

Методы, основанные на **резервировании времени**, сводятся к выделению интервалов времени (слотов), которые распределяются между узлами. Узел получает канал в свое распоряжение на всю длительность выделенных ей слотов. Существуют варианты методов, учитывающие приоритеты – узлы с более высоким приоритетом получают большее количество слотов.

Кольцевые методы используются в ЛВС с кольцевой топологией. Кольцевой метод вставки регистров заключается в подключении параллельно к кольцу одного или нескольких буферных регистров. Данные для передачи за-

писываются в регистр, после чего узел ожидает межкадрового промежутка. Затем содержимое регистра передается в канал. Если во время передачи поступает кадр, он записывается в буфер и передается после своих данных.

Различают клиент-серверные и одноранговые методы доступа. **Клиент-серверные** методы доступа предполагают наличие в сети центрального узла, управляющего всеми остальными. Такие методы распадаются на две группы: с опросом и без опроса.

Среди методов доступа с опросом наиболее распространены “опрос с остановкой и ожиданием” и “непрерывный автоматический запрос на повторение” (ARQ). В любом случае первичный узел последовательно передает узлам разрешения на передачу данных. Если узел имеет данные для передачи, он выдает их в среду передачи, если нет – либо выдает короткий пакет данных типа “данных нет”, либо просто ничего не передает.

При использовании **одноранговых** методов доступа все узлы равноправны. Мультиплексная передача с временным разделением – наиболее простая одноранговая система без приоритетов, использующая жесткое расписание работы узлов. Каждому узлу выделяется интервал времени, в течение которого узел может передавать данные, причем интервалы распределяются поровну между всеми узлами.

7.2.1. Метод доступа с контролем несущей и определением коллизий

Множественный доступ с контролем несущей и определением коллизий (CSMA/CD, Carrier Sense Multiple Access/Collision Detect) – наиболее распространенный метод случайного доступа из применяющихся в локальных сетях. Все узлы сети постоянно прослушивают канал (контроль несущей). Если узел имеет данные для передачи, он дожидается тишины в канале и начинает передачу. При этом может оказаться так, что другой узел тоже обнаружил, что канал свободен и тоже начал передачу. Такая ситуация называется коллизией. Поскольку все узлы, передавая данные, продолжают прослушивать канал, они могут обнаружить наложение сигналов от разных источников. При обнаружении коллизии передающие узлы выдают в канал специальную последовательность битов – “затор”, служащий для оповещения остальных узлов о коллизии. Затем все передающие узлы прекращают передачу и планируют ее на более позднее время. Величина паузы выбирается случайным образом.

7.2.2. Маркерные методы доступа

Метод передачи маркера относится к селективным детерминированным одноранговым методам доступа. Сети с шинной топологией, использующие передачу маркера, называются сетями типа “маркерная шина” (token bus), а кольцевые сети – сетями типа “маркерное кольцо” (token ring).

В сетях типа “маркерная шина” маркер представляет собой кадр, содержащий поле адреса, в которое записывается адрес узла, которой предоставляет-

ся право доступа к среде передачи. После передачи кадра данных, передающий узел записывает в маркер адрес следующего узла и выдает маркер в канал.

Сети типа “маркерное кольцо”, являясь сетями с кольцевой топологией, обладают последовательной конфигурацией: каждая пара узлов связана отдельным каналом, а для функционирования сети необходимо функционирование всех узлов. В таких сетях маркер не содержит адреса узла, которому разрешена передача, а содержит только поле занятости, которое может содержать одно из двух значений: “занят” и “свободен”. Когда узел, имеющий данные для передачи, получает свободный маркер, он меняет состояние маркера на “занят”, а затем передает в канал маркер и свой кадр данных. Станция-получатель, распознав свой адрес в кадре данных, считывает предназначенные ей данные, но не меняет состояния маркера. Изменяет состояние маркера на “свободен” (после полного оборота маркера с кадром данных по кольцу) тот узел, который его занял. Кадр данных при этом удаляется из кольца. Узел не может повторно использовать маркер для передачи другого кадра данных, а должен передать свободный маркер дальше по кольцу и дождаться его получения после одного или нескольких оборотов.

Равноранговые приоритетные системы включают приоритетные слотовые системы, системы с контролем несущей без коллизий и системы с передачей маркера с приоритетами.

Приоритетные слотовые системы подобны системам с мультиплексной передачей с временным разделением, но выдача слотов происходит с учетом приоритетов узлов. Критериями для установления приоритетов могут являться: предшествующее владение слотом, время ответа, объем передаваемых данных и др.

Системы с контролем несущей без коллизий (CSMA/CA, Carrier Sense Multiple Access/Collision Avoidance) отличаются от систем с обнаружением коллизий наличием у узлов таймеров, определяющих безопасные моменты передачи. Длительности таймеров устанавливаются в зависимости от приоритетов узлов: станции с более высоким приоритетом имеют меньшую длительность таймера.

Приоритетные системы с передачей маркера определяют приоритеты узлов таким образом, что чем меньше номер узла, тем выше его приоритет. Маркер при этом содержит поле резервирования, в которое узел, собирающийся передавать данные, записывает свое значение приоритета. Если в кольце встретится узел с более высоким приоритетом, который тоже имеет данные для передачи, этот узел запишет свое значение приоритета в поле резервирования, чем перекроет предыдущую заявку (сохранив старое значение поля резервирования в своей памяти). Если маркер, поступивший на узел, содержит в поле резервирования значение приоритета данного узла, данный узел может передавать данные. После оборота маркера по кольцу и его освобождения, передававший узел должен восстановить в маркере значение поля резервирования, сохраненное в памяти.

8. ТЕХНОЛОГИЯ ETHERNET

8.1. Стандарты группы IEEE 802

Комитет 802 института IEEE был создан в 1980 году с целью выработки стандартов для локальных сетей. Результаты работы этого комитета (группа стандартов IEEE 802.x) легли в основу международных стандартов от ISO 8802-1 до ISO 8802-5. Комитет 802 не столько разрабатывал новые протоколы, сколько выделял в широко распространенных фирменных технологиях общие принципы, подходы и функции, и формулировал открытые стандарты на их основе. Группа стандартов IEEE 802.x охватывает два нижних уровня модели ВОС – физического и канального уровня. Канальный уровень с точки зрения стандартов 802.x состоит из двух подуровней:

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

Подуровень LLC предоставляет стандартный интерфейс с сетевым уровнем, независимый от сетевой технологии. Протоколы сетевого уровня, когда им нужно передать кадр данных, обращаются именно к подуровню LLC.

Подуровень MAC обеспечивает совместное использование среды передачи, выполняя соответствующие алгоритмы доступа. Специфические особенности технологий локальных сетей – Ethernet, Token Ring, FDDI, Fast Ethernet, 10VG-AnyLAN и др. – реализуются именно на подуровне MAC.

Часть стандартов группы 802 описывает отдельные технологии, а часть содержит стандарты, общие для разных технологий.

Подгруппа 802.1 содержит общие определения локальных сетей, связь модели IEEE 802 с моделью OSI, правила взаимодействия различных технологий.

К ней относятся:

- 802.1d – логика работы моста/коммутатора; алгоритм покрывающего дерева.
- 802.1h – логика работы транслирующего моста (связывающего сети разных технологий).
- 802.1p – дополнения к логике мостов для работы с трафиком разных приоритетов и выполнения динамической фильтрации группового вещания.
- 802.1q – построение виртуальных локальных сетей (Virtual LAN, VLAN) с помощью мостов/коммутаторов.

Стандарт 802.2 описывает работу подуровня LLC.

Подгруппа стандартов 802.3 описывает работу подуровня MAC и физического уровня с методом доступа CSMA/CD. Собственно стандарт 802.3 определяет технологию Ethernet (10 Мбит/с), 802.3u – Fast Ethernet (100 Мбит/с), 802.3z и 802.3ab – Gigabit Ethernet (1 Гбит/с). Стандарт 802.3x определяет правила управления потоком для дуплексного режима.

Стандарт 802.4 описывает работу подуровня MAC и физического уровня технологий типа маркерная шина (Token Ring, протокол MAP (Manufacturing Automation Protocol) для связи устройств промышленной автоматике).

Стандарт 802.5 описывает работу подуровня MAC и физического уровня технологий типа маркерного кольца (Token Ring).

Стандарт 802.6 описывает городские сети (Metropolitan Area Network, MAN).

Стандарт 802.7 описывает принципы широкополосной передачи.

Стандарт 802.8 описывает принципы построения сетей на основе волоконно-оптических технологий.

Стандарт 802.9 содержит совместимые с ISDN спецификации совместной передачи голоса и данных.

Стандарт 802.10 описывает принципы сетевой безопасности.

Стандарт 802.11 описывает беспроводные технологии передачи данных.

Стандарт 802.12 определяет технологию передачи с методом доступа по требованию с приоритетами (100VG-AnyLAN).

8.2. Протокол управления логическим каналом IEEE 802.2

Стандарт 802.2 описывает работу подуровня LLC – логические процедуры передачи кадров и связь с сетевым уровнем. Стандарт определяет три типа обслуживания:

- LLC1 – без установления соединения и подтверждений
- LLC2 – с установлением соединения и подтверждениями
- LLC3 – без установления соединения и с подтверждениями.

Процедура обслуживания LLC1 передает данные в дейтаграммном режиме, минимизируя издержки за счет надежности. Эта процедура используется, когда протоколы верхних уровней сами обеспечивают требуемую надежность.

Процедура обслуживания LLC2, прежде чем передавать данные, устанавливает логическое соединение с получателем, выполняет упорядочение потока данных и перезапрос пропущенных блоков данных. Подтверждения обрабатываются в режиме скользящего окна. Применяется для обеспечения надежной передачи данных на линиях с высоким уровнем ошибок.

Процедура обслуживания LLC3 не устанавливает логическое соединение, но требует передачи подтверждений приема данных. Используется в ситуациях, когда издержки на установление соединения недопустимы, а контроль доставки данных необходим (например, в системах управления реального времени).

Кадры LLC состоит из заголовка и поля данных. При передаче подуровню MAC кадр LLC обрамляется двумя однобайтовыми полями со значением 01111110. Заголовок содержит три поля:

- DSAP (Destination Service Access Point, точка доступа к сервису назначения)
- SSAP (Source Service Access Point, точка доступа к сервису источника)
- Control (управление).

Поля DSAP и SSAP занимают по 1 байту и идентифицируют протокол верхнего уровня, который отправил кадр (SSAP), и которому этот кадр предназначен (DSAP). Возможные значения этих полей определены в стандарте 802.2.

Например, протоколу IP соответствует значение 0x06, а протоколу NetBIOS – 0xF0.

Поле Control задает тип кадра и, возможно, несет дополнительную информацию. Размер этого поля может составлять 1 или 2 байта.

Каждый кадр LLC относится к одному из трех типов (в зависимости от значения старших битов поля Control):

- нумерованный (Unnumbered) – поле Control занимает 1 байт, два старших бита имеют значение 11,
- информационный (Information) – поле Control занимает 2 байта, старший бит установлен в 0,
- управляющий (Supervisory) – поле Control занимает 2 байта, два старших бита имеют значение 10.

Структура поля Control для разных типов кадров приведена на рис.8.1.

Тип кадра	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ненумерованный	1	1	M		P/F	M										
Информационный	0				N(S)			P/F		N(R)						
Управляющий	1	0	S	-	-	-	-	N(R)								

Рис.8.1. Структура поля Control кадра LLC

Процедура LLC1 использует только ненумерованные кадры с нулевым значением всех подполей (кроме двух первых бит). Поскольку протокол Ethernet использует обратный порядок бит в байте, то значение поля Control кадров LLC1, используемых в сетях Ethernet, имеет значение 0x03.

Процедура LLC2 использует кадры всех типов. Кадры делятся на команды и ответы. Разряд P/F в командах называется Poll (запрос) и требует, чтобы на команду был дан ответ, а в ответах называется F (Final) и указывает на последний кадр в ответе. Ненумерованные кадры используются для установления соединения, их поле M несет код команды – запрос установки соединения, подтверждение соединения, разрыв соединения. После того, как соединение установлено, передача пользовательских данных и подтверждений осуществляется кадрами информационного типа. Поле N(S) несет номер отправленного кадра, поле N(R) несет номер кадра, который ожидает получить узел-источник. Поскольку поля N(S) и N(R) имеют длину в семь битов, для нумерации кадров циклически используются числа от 0 до 127. Если поступает кадр с номером, отличным от того, который ожидался приемником (например, после кадра 56 приходит кадр 58, а не ожидаемый кадр 57), такой кадр отбрасывается и передатчику отправляется кадр управляющего типа с кодом отказа в поле S и указанием ожидаемого номера кадра в поле N(R). Передатчик при этом должен возобновить передачу, начиная с запрошенного кадра.

Управляющие кадры, помимо передачи отказа (Reject, REJ), могут передавать еще две команды: **приемник не готов** (Receiver Not Ready, RNR) и **приемник готов** (Receiver Ready, RR), используемые для управления потоком. Если приемник не успевает обработать поток кадров, он отправляет управляющий кадр с командой RNR, по которой передатчик должен приостановить передачу до получения кадра с командой RR.

8.3. Технология Ethernet

Технология Ethernet была разработана в исследовательском центре компании Херох в середине 1970-х годов. В 1980 году фирмы DEC, Intel и Херох выпустили вторую фирменную версию стандарта Ethernet (Ethernet DIX или Ethernet II). На основе Ethernet DIX был разработан стандарт 802.3. Эти два стандарта очень близки, но есть и некоторые отличия, например, в формате кадра. В настоящее время термин Ethernet обычно используется для описания всех локальных сетей, использующих метод доступа с контролем несущей и обнаружением коллизий (CSMA/CD, Carrier Sense Multiple Access/Collision Detection).

8.4. Метод доступа CSMA/CD

Метод доступа CSMA/CD определяет, во-первых, каким образом станция определяет момент, когда она может передать кадр, во-вторых – каким образом должны вести себя станции в случае одновременного начала передачи кадров двумя или более узлами.

Каждая станция постоянно прослушивает сеть. Если в сети присутствует сигнал несущей частоты, значит, другая станция передает свой кадр. Для того, чтобы иметь право передать кадр, станция должна дождаться “тишины” (отсутствия несущей), выждать технологическую паузу (9.6 мкс), и, если за время паузы сигнал несущей не появился, начать передачу.

Все станции, прослушивая сеть, распознают передаваемый кадр, и та из них, чей адрес записан в поле получателя, принимает кадр полностью и передает его протоколам верхних уровней. Остальные станции “чужие” кадры должны игнорировать.

Возможна ситуация, когда две станции одновременно начинают передачу кадров. Такая ситуация называется **коллизией** (collision). Наступление коллизии передающая станция может определить по отличию передаваемых и принимаемых ею данных (во время передачи кадра станция продолжает прослушивать сеть). Обнаружившая коллизию станция должна прекратить передачу кадра, передать в сеть специальный сигнал затора (jam), состоящий из 32 бит, и выдерживает паузу случайной длительности (определяемой по специальному алгоритму). После этого она может опять попытаться передать свой кадр (естественно, дождавшись “тишины” и выждав технологическую паузу).

Интервал времени до повторной попытки доступа после коллизии определяется как случайное число интервалов отсрочки (один интервал отсрочки равен 512 битовым интервалам, т.е. 51,2 мкс). Количество интервалов отсрочки определяется как случайное целое число, равномерно распределенное в интервале $0..2^n$ ($1 \leq n \leq 10$) или $0..2^{10}$ ($10 < n \leq 16$). Здесь n – номер попытки передачи кадра. Если 16 попыток заканчиваются неудачно (порождая коллизии), подуровень MAC отбрасывает кадр и передает верхним уровням сообщение об ошибке.

8.5. Время двойного оборота

Основным принципиальным ограничением на параметры сети (диаметр сети, размер пакета и др.) является необходимость надежного распознавания коллизий. Станция, передающая пакет, может определить наступление коллизии только во время передачи кадра. Значит, максимальный диаметр сети должен быть таков, чтобы за время передачи кадра минимальной длины первый его бит успел достичь самой дальней станции и вернуться (возможно, искаженным) обратно. Если искаженный первый бит вернется уже после окончания передачи пакета, передававшая станция не сможет распознать коллизию. Если T_{min} – время передачи кадра минимальной длины, а RTT – **время двойного оборота** (round trip time, время, за которое сигнал проходит дважды между наиболее удаленными станциями), то должно выполняться соотношение: $T_{min} \geq RTT$. Ограничения на размер сети в Ethernet параметры подобраны таким образом, чтобы коллизии гарантированно распознавались.

8.6. Форматы кадров Ethernet

В сетях Ethernet могут применяться кадры четырех форматов:

- Ethernet II (Ethernet DIX)
- Ethernet 802.2
- Ethernet 802.3
- Ethernet SNAP.

На рис.8.2. приведены форматы кадров (первая строка – обозначения полей, вторая строка – размеры полей в байтах).

Кадр Ethernet II										
P	DA	SA	Type	Data					FCS	
8	6	6	2	46-1500					4	

Кадр Ethernet 802.2 (802.3+802.2)										
P	SFD	DA	SA	Length	DSAP	SSAP	Control	Data		FCS
7	1	6	6	2	1	1	1/2	43/42-1497/1496		4

Кадр Ethernet 802.3 ("Raw")										
P	SFD	DA	SA	Length	Data					FCS
7	1	6	6	2	46-1500					4

Кадр Ethernet SNAP										
P	SFD	DA	SA	Length	DSAP (0xAA)	SSAP (0xAA)	Control (0x03)	ProtID	Data	FCS
7	1	6	6	2	1	1	1	5	38-1492	4

Рис.8.2. Форматы кадров Ethernet

Поле P (Preamble, преамбула) состоит из семи байт 10101010 и используется для синхронизации. Преамбула кадра Ethernet II содержит также поле SFD.

Поле SFD (Start of Frame Delimiter, разделитель начала кадра) имеет значение 10101011 и указывает на то, что следующий байт принадлежит заголовку кадра.

Поле DA (Destination Address, адрес назначения) содержит адрес одного из трех типов:

- индивидуальный (unicast) адрес – первый бит старшего байта равен 0, указывает на единственного получателя (представляет собой его MAC-адрес); уникальность адресов обеспечивают производители сетевого оборудования: во втором и третьем байте хранится номер фирмы-изготовителя, а остальные заполняются изготовителем; некоторые сетевые адаптеры позволяют устанавливать для них произвольный MAC-адрес;
- широковещательный (broadcast) адрес – состоит из всех единиц (0xFFFFFFFF), указывает на то, что данный кадр должен быть получен всеми узлами сети;
- групповой (multicast) адрес – первый бит старшего байта равен 1, в остальных битах хранится номер группы узлов, для которых предназначен данный кадр.

Поле SA (Source Address, адрес источника) содержит MAC-адрес отправителя кадра (всегда индивидуальный адрес).

Поле Type (тип) указывает на протокол верхнего уровня, чьи данные передаются в кадре (фактически, выполняет функции полей DSAP и SSAP из заголовка кадра LLC).

Поле Length (длина) содержит размер поля Data (в байтах).

Поле Data (данные) содержит данные, переданные протоколом верхнего уровня.

Поле FCS (Frame Check Sequence, контрольная последовательность кадра) содержит контрольную сумму кадра, вычисленную по алгоритму CRC-32.

Поля DSAP, SSAP и Control составляют заголовок LLC-кадра.

Поле ProtID (идентификатор протокола) позволяет использовать кадры Ethernet для передачи данных более широкого множества протоколов верхнего уровня. Это поле состоит из двух под полей: трехбайтного OUI (Organizationally Unique Identifier, организационно-уникальный идентификатор), хранящего номер организации, контролирующей коды протоколов во втором (двухбайтном) подполе Type (тип). IEEE присвоил OUI = 0x00000.

8.7. Пропускная способность сети Ethernet

Пропускная способность оценивается через количество кадров либо количество байт данных, передаваемых по сети за единицу времени. Если в сети не происходят коллизии, максимальная скорость передачи кадров минимального размера (64 байта) составляет 14881 кадров в секунду. При этом полезная пропускная способность для кадров типа 802.2 и SNAP составляет 4.4 Мбит/с, а для кадров Ethernet II и 802.3 – 5.48 Мбит/с. Максимальная скорость передачи

кадров максимального размера (1500 байт) составляет 813 кадров в секунду. Полезная пропускная способность при этом составит 9.76 Мбит/с.

9. СЕТИ TOKEN RING И FDDI

9.1. Технология Token Ring

Технология Token Ring (маркерное кольцо) была разработана фирмой IBM в конце 1970-х годов. Спецификации IEEE 802.5 практически повторяют фирменные спецификации, отличаясь лишь в некоторых деталях (например, IEEE 802.5 не оговаривает среду передачи и топологию сети, а фирменный стандарт определяет витую пару в качестве среды и звезду в качестве физической топологии). Сети Token Ring могут работать на одной из двух битовых скоростей: 4 Мбит/с (IEEE 802.5) или 16 Мбит/с (IEEE 802.5r). В одном кольце могут присутствовать только станции, работающие на одной скорости.

Token Ring определяет логическую топологию “кольцо”: каждая станция связана с двумя соседними. Физически же станции соединяются в звездообразную сеть, в центре которой находится **устройство многостанционного доступа** (MSAU, Multi-Station Access Unit), по сути представляющее собой повторитель. Как правило, MSAU умеет исключать неработающую станцию из кольца (для этого используется шунтирующее реле). MSAU имеют также отдельные разъемы для объединения нескольких MSAU в одно большое кольцо. Максимальное количество станций в кольце – 250 (IEEE 802.5), 260 (IBM Token Ring, кабель STP) и 72 (IBM Token Ring, кабель UTP).

Максимальная длина кольца Token Ring составляет 4000 м.

В конце 1990-х годов компанией IBM разработан новый вариант технологии Token Ring – High Speed Token Ring (HSTR), поддерживающий скорости в 100 и 155 Мбит/с. Ведутся разработки версии Token Ring со скоростью в 1 Гбит/с.

9.1.1. Маркерный метод доступа

Token Ring – это наиболее распространенная технология локальной сети с передачей маркера. В таких сетях циркулирует (передается станциями друг другу в определенном порядке) специальный блок данных – **маркер** (token). Станция, принявшая маркер, имеет право передавать свои данные. Для этого она изменяет в маркере один бит (“маркер занят”), добавляет к нему свои данные и передает в сеть (следующей станции). Станции передают такой кадр дальше по кольцу, пока не достигнет получателя, который скопирует из него данные и передаст дальше. Когда отправитель получает свой кадр с данными совершивший полный круг, он его отбрасывает и либо передает новый кадр данных (если не истекло максимальное время владения маркером), либо изменяет бит занятости маркера на “свободен” и передает маркер дальше по кольцу.

В течение всего времени обладания маркером, до и после передачи своего кадра, станция должна выдавать заполняющую последовательность (fill se-

quence) – произвольную последовательность 0 и 1. Это делается для поддержания синхронизации и контроля за обрывом кольца.

Основной режим работы адаптера – повторение: передатчик побитно выдает данные, поступившие к приемнику. Когда у станции есть кадр для передачи и принят свободный маркер, станция переходит в режим передачи, при этом поступающий через приемник битовый поток анализируется на служебные кадры и либо (если обнаружен служебный кадр) инициируется прерывание (прекращение передачи своего кадра и выдача кадра прерывания), либо принятые данные отбрасываются.

В сетях Token Ring 4 Мбит/с станция освобождает маркер только после возвращения ее кадра данных. Сети Token Ring 16 Мбит/с используют алгоритм **раннего освобождения маркера** (Early Token Release): маркер передается в кольцо сразу по окончании передачи кадра данных. При этом по кольцу одновременно передается несколько кадров данных, но генерировать их в каждый момент времени может только одна станция – владеющая в этот момент маркером.

За правильной работой сети следит активный монитор (Active Monitor, АМ), выбираемый во время инициализации кольца как станция с максимальным MAC-адресом. В случае отказа активного монитора, проводятся выборы нового (все станции в сети, кроме активного монитора, считаются резервными мониторами (Standby monitor)). Основная функция активного монитора – контроль наличия единственного маркера в кольце. Монитор выпускает в кольцо маркер и удаляет кадры, прошедшие больше одного оборота по кольцу. Чтобы сообщить другим станциям о себе, активный монитор периодически передает служебный кадр АМР. Если за некоторое время (достаточное для оборота маркера по кольцу) маркер не вернется к активному монитору, маркер считается утерянным, и активный монитор генерирует новый маркер.

На режим передачи кадров влияют определенные в стандарте максимальные интервалы времени, за соблюдением которых следят специальные таймеры в сетевых адаптерах (приведены значения по умолчанию, администратор сети может их изменять):

- время удержания маркера (Token Holding, ТНТ) – 8,9 мс; по истечении этого интервала станция должна прекратить передачу своих данных (текущий кадр можно передать) и освободить маркер; за время удержания маркера станция может передать несколько (небольших) кадров;
- допустимое время передачи кадра (Valid Transmission, TVX) – 10 мс; максимальное время, в которое должна уложиться передача одного кадра; контролируется активным монитором;
- время ожидания свободного маркера (No Token, ТНТ) – 2,6 с; время ожидания свободного маркера активным монитором; если за это время маркер не появится, активный монитор выполняет очистку кольца и генерирует новый маркер;
- период посылки АМР (Active Monitor, ТАМ) – 7 с;

- время ожидания AMP (Standby Monitor Detect AMP, TSM) – 16 с; если за этот интервал не было ни одного кадра AMP, инициируются выборы нового активного монитора.

Форматы кадров Token Ring

Token Ring определяет три типа кадров: маркер, кадр данных (служебных или пользовательских) и прерывание.

Маркер

Поле	SD	AC	ED
Длина (байт)	1	1	1

Кадр данных

Поле	SD	AC	FC	DA	SA	RI	Info	FCS	ED	FS
Длина (байт)	1	1	1	6	6	≥ 0	≥ 0	4	1	1

Прерывание

Поле	SD	ED
Длина (байт)	1	1

Рис.9.1. Форматы кадров Token Ring

Поле SD (Starting Delimiter, начальный ограничитель) указывает на начало кадра и имеет значение JK0JK000 в манчестерском коде. Поскольку в поле присутствуют специальные коды J и K, последовательность данных нельзя спутать с ограничителем кадра.

Поле ED (Ending Delimiter, конечный ограничитель) имеет значение JK1JK1E, где бит I (Intermediate, промежуточный) указывает, является ли кадр промежуточным в последовательности кадров (I=1) или последним/единственным (I=0), а бит E (Error, ошибка) указывает на обнаруженную ошибку (E=1).

Поле AC (Access Control, управление доступом) имеет формат PPRTMRRR, где биты PPP (Priority, приоритет) содержат приоритет маркера, бит T (Token, маркер) отличает свободный маркер (T=1) от кадра данных (T=0), бит M (Monitor, монитор) используется для распознавания кадров, совершивших более одного оборота по кольцу: монитор устанавливает M=1 во всех проходящих через него кадрах (остальные станции устанавливают M=0), а кадры с M=1 должен удаляться монитором. Биты RRR (Priority reservation, резервирование) несут приоритет станции, желающей захватить маркер.

Поле FC (Frame Control, управление кадром) имеет формат FFZZZZZZ. Биты FF определяют тип кадра:

- 00 – кадр данных со служебной информацией (MAC-кадр)
- 01 – кадр данных пользователя (LLC-кадр)
- 10, 11 – резерв.

Биты ZZZZZZ используются LLC-кадрами для хранения информации о приоритете кадра уровня LLC. MAC-кадры в этих битах хранят свой тип. IEEE 802.5 определяет 25 типов MAC-кадров, среди которых основные:

- CT (Claim Token, заявка на создание маркера) – отправляется резервным монитором при подозрении об отказе активного монитора;
- DAT (Duplicate Address Test, тест на дублирование адреса) – отправляется станцией при подключении к кольцу для проверки уникальности своего адреса;
- AMP (Active Monitor Present, присутствует активный монитор) – регулярно (раз в 7 с) отправляется активным монитором для подтверждения своего присутствия;
- SMP (Standby Monitor Present, присутствует резервный монитор) – ответ на кадр AMP;
- BCN (Beacon, бакен) – отправляется станцией, обнаружившей сетевую проблему (тишину или нескончаемый поток, что может указывать на обрыв кабеля, наличие неисправного адаптера у одной из станций и т.п.);
- PRG (Purge, очистка) – сигнал от активного монитора об очистке кольца от всех кадров.

Поле DA (Destination Address, адрес назначения) имеет структуру, подобную структуре адреса в стандарте IEEE 802.3. Старший бит адреса определяет получателя: 0 – индивидуальный (одна станция), 1 – групповой. Второй бит адреса определяет способ назначения адреса: 0 – глобально (универсально, зашифто в ПЗУ адаптера), 1 – локально. Остальные биты используются для указания адреса станции, кольца или группы получателей. Несколько адресов зарезервировано для служебных целей:

FF FF FF FF FF FF – широковещательный кадр (всем станциям)

C0 00 FF FF FF FF – широковещательный MAC-кадр

C0 00 00 00 00 01 – активный монитор

C0 00 00 00 00 02 – сервер параметров кольца

C0 00 00 00 00 08 – монитор ошибок кольца

C0 00 00 00 00 10 – сервер отчетов о конфигурации

C0 00 00 00 01 00 – мост

C0 00 00 00 20 00 – управление сетью.

Поле SA (Source Address, адрес источника) имеет тот же формат, что и адрес назначения, за исключением старшего бита. В адресе источника старший бит называется RII (Routing Information Indicator) и указывает (если RII=1) на наличие данных в поле RI.

Поле RI (Routing Information, маршрутная информация), если используется (RII=1), содержит последовательность (двухбайтных) адресов сегментов на пути к получателю. Данные этого поля управляют работой мостов в режиме маршрутизации от источника.

Поле Info содержит либо данные пользователя (кадр LLC), либо служебные данные, определяемые типом кадра (кадр MAC). Стандарт не ограничивает размер этого поля, хотя практически его максимальный размер определяется соотношением времен передачи кадра и удержания маркера. Для 4 Мбит/с мак-

симальный размер кадра обычно устанавливается в 4 Кбайт, а для 16 Мбит/с – в 16 Кбайт. Минимальный размер поля данных не определен.

Поле FCS (Frame Check Sequence, контрольная сумма) хранит 4-байтный CRC-код для всех полей с FC по Info включительно.

Поле FS (Frame Status, статус кадра) имеет формат AСтгАСтг. Биты гг резервированы и не используются, остальные биты дублируются для надежности. Бит А (Address Recognized, адрес распознан) указывает на то, что получатель кадра присутствует в кольце, а бит С (Frame Copied, кадр скопирован) указывает на то, что приемник скопировал кадр себе в буфер. По этим полям станция-отправитель может узнать, что переданный ею кадр был получен.

9.1.2. Система приоритетного доступа

Сети Token Ring гарантируют, что каждая станция будет получать право на передачу данных не реже, чем раз в установленный интервал времени. Кроме того, используется система приоритетов, позволяющая некоторым станциям пользоваться сетью чаще других. Для этого в кадре Token Ring выделено два поля: поле приоритета и поле резервирования. Всего уровней приоритета восемь: от низшего (0) до высшего (7). Маркер тоже всегда имеет некоторый уровень приоритета. Станция может захватить маркер только в том случае, если приоритет кадра, который она собирается передать, не ниже приоритета маркера (битов PPP поля AC).

Станция, захватившая маркер, сохраняет старое значение его приоритета, записывает в него приоритет своего кадра и обнуляет поле резервирования. Если в кольце есть станция, желающая передать кадр с более высоким приоритетом, то она записывает приоритет своего кадра в поле резервирования проходящего по кольцу кадра, в результате чего после оборота по кольцу в поле резервирования будет записан максимальный приоритет из кадров, ожидающих передачи. Тогда станция переписывает приоритет из поля резервирования в поле приоритета маркера и выдает свободный маркер в кольцо (захватить такой маркер сможет только станция с кадром указанного приоритета).

Станция, повышающая приоритет маркера, становится запоминающей станцией (stacking station) и организует стек для хранения еще не обслуженных низких приоритетов. Когда через такую станцию проходит свободный маркер с приоритетом, равным приоритету на верхушке стека, она извлекает следующее значение из стека и понижает приоритет маркера до него.

Механизм приоритетов в сетях Token Ring не является обязательным к использованию. Как правило, большинство приложений им не пользуется, и кольцо работает в неприоритетном режиме (приоритет маркера всегда равен 0). Существует тенденция к переносу механизмов приоритетного обслуживания на уровни, выше канального (приоритетное обслуживание могут обеспечивать, например, маршрутизаторы).

9.1.3. Оборудование Token Ring

Концентратор Token Ring (MSAU) представляет собой набор блоков TCU (Trunk Coupling Unit – блок подключения к магистрали), к которым отдельными радиальными кабелями (lobe cabling) подключаются станции. Блок TCU содержит реле, в нормальном состоянии замыкающее магистраль в обход порта (одновременно замыкает вход и выход порта со стороны станции). Если к порту подключена станция, то она выдает “фантомный” сигнал постоянного тока, переключающий реле. Если станция отключается от кольца или происходит обрыв кабеля, реле восстанавливает обходной путь. Станция, физически подключенная к TCU, может проверить свою линию до MSAU (поскольку TCU обеспечивает замыкание ее приемника на ее передатчик), и, в случае исправности линии, выдать “фантомный сигнал”.

Кроме блоков TCU (обычно от 8 до 24), концентраторы MSAU имеют два порта для образования кольца концентраторов: порт RI (Ring In, вход кольца) и порт RO (Ring Out, выход кольца). Эти порты также снабжены реле, обеспечивающим замыкание магистрали в обход отключенного порта.

Концентраторы могут быть пассивными и активными. Пассивный MSAU обеспечивает только электрическое подключение станции к магистрали. Активный MASU имеет в каждом блоке TCU повторитель, восстанавливающий форму сигнала. Активные концентраторы могут содержать блок управления по SNMP или RMON. Сегментирующие (Port switch) концентраторы позволяют организовывать несколько колец на одном устройстве.

Сетевые адаптеры содержат блок повторения, который может регенерировать сигнал и восстанавливать его синхронизацию (этим занимается только активный монитор). Для ресинхронизации используется 30-битный буфер, в котором накапливаются сигналы. Этот буфер подключается активным монитором к кольцу, и все данные пропускаются через него, выходя с нужной частотой. (При максимальном количестве станций (260) смещение бита за оборот по кольцу может достигать трех битовых интервалов.)

Технология Token Ring позволяет использовать для магистральных и радиальных кабелей витую пару (UTP или STP) или оптоволокно. Расстояние между пассивными концентраторами может достигать 100 м (STP Type 1) и 45 м (UTP Category 3), а между активными – 730 м и 365 м соответственно. Использование оптоволокна увеличивает максимальную длину каждого сегмента до 1 км. Разные производители оборудования и программного обеспечения определяют различные ограничения, так что при проектировании сети Token Ring необходимо пользоваться данными выбранного производителя.

9.2. Технология FDDI

Спецификация FDDI (Fiber Distributed Data Interface, оптоволоконный интерфейс распределения данных) разработана и стандартизована институтом ANSI (в 1986-1988 гг. – группа X3T9.5, после 1995 года – группа X3T12). FDDI – это исторически первая технология локальных сетей, использующая в качестве среды передачи оптоволоконный кабель. Начальные версии FDDI обеспечивают скорость передачи 100 Мбит/с по двойному оптоволоконному кольцу

длиной до 100 км. В нормальном режиме данные передаются только по одному кольцу из пары – первичному (primary). Вторичное (secondary) кольцо используется в случае отказа части первичного кольца. По первичному и вторичному кольцам данные передаются в противоположных направлениях, что позволяет сохранить порядок узлов сети при подключении вторичного кольца к первичному. В случае нескольких отказов, сеть FDDI распадается на несколько отдельных (но функционирующих) сетей.

Технология обеспечивает передачу синхронного и асинхронного трафика: синхронный трафик передается всегда, независимо от загруженности кольца, асинхронный трафик может произвольно задерживаться. Каждой станции выделяется часть полосы пропускания, в пределах которой станция может передавать синхронный трафик. Остающаяся часть полосы пропускания кольца отводится под асинхронный трафик. Сети FDDI не определяют приоритетов для кадров, любой приоритетный трафик должен передаваться, как синхронный, а остальные данные – асинхронно.

FDDI использует маркерный метод доступа, близкий к методу доступа сетей Token Ring. Основное отличие – в плавающем значении времени удержания маркера для асинхронного трафика: при небольшой загрузке сети время удержания растет, а при перегрузках – уменьшается. Во время инициализации кольца узлы договариваются о максимально допустимом времени оборота маркера по кольцу T_{Opr} . Для синхронного трафика время удержания маркера не изменяется. Для передачи синхронного кадра узел всегда имеет право захватить проходящий маркер и удерживать его в течении заранее заданного фиксированного времени. Если узел хочет передать асинхронный кадр, он должен измерить время оборота маркера (Token Rotation Time, TRT) – интервал между двумя прохождениями маркера через него. Если кольцо не перегружено ($TRT < T_{Opr}$), то узел может захватить маркер и передать свой кадр (или кадры) в кольцо, при этом допустимое время удержания маркера $THT = T_{Opr} - TRT$. Если кольцо перегружено ($TRT > T_{Opr}$), то узел не имеет права захватывать маркер.

Как и сети Token Ring 16 Мбит/с, FDDI использует алгоритм раннего освобождения маркера, в результате чего в кольце одновременно может продвигаться несколько кадров (маркер всегда один). Формат кадра FDDI очень близок к формату кадра Token Ring, за исключением полей приоритета.

Стандарт FDDI определяет четыре компонента:

- MAC (Media Access Control), определяющий форматы кадров, манипуляции с маркером, адресацию, обработку ошибок при логических отказах (соответствует канальному уровню модели OSI);
- PHY (Physical) выполняет физическое и логическое кодирование и декодирование, синхронизацию и кадрирование;
- PMD (Physical Medium Dependent) определяет свойства оптических или электрических компонентов, параметры линий связи (PMD и PHY соответствуют физическому уровню OSI);
- SMT (Station Management) выполняет все функции по управлению и контролю работы остальных компонентов, определяет конфигурацию узлов и ко-

лец, процедуры подключения/отключения, изоляцию отказавших элементов, обеспечивает целостность кольца (подключая вторичное кольцо при отказе первичного).

В качестве среды передачи FDDI может использовать многомодовое оптоволокно (MMF-PMD, длина кабельного сегмента до 2 км), одномодовое оптоволокно (SMF-PMD) витую пару категории 5 или экранированную витую пару STP Type 1 (TP-PMD). Все оптоволоконные варианты FDDI используют длину волны 1300 нм. Разновидность FDDI на витой паре иногда называют CDDI (Copper Distributed Data Interface) или TPDDI (Twisted Pair Distributed Data Interface).

FDDI использует отдельные линии для передачи и приема сигналов. Логическое кодирование – 4B/5B. Физическое кодирование при использовании оптоволокна – NRZI, при использовании витой пары – MLT-3.

Технология FDDI достаточно легко интегрируется с Ethernet и Token Ring, в результате чего часто используется в качестве высокоскоростной магистрали, объединяющей эти сети, а также для высокоскоростного подключения серверов.

В последнее время, эту нишу у FDDI отвоевывают более дешевые высокоскоростные модификации Ethernet – Fast Ethernet и Gigabit Ethernet, но они не могут гарантировать сравнимые с FDDI отказоустойчивость и расстояния между узлами.

10. ВЫСОКОСКОРОСТНЫЕ ТЕХНОЛОГИИ ЛОКАЛЬНЫХ СЕТЕЙ

10.1. Технология Fast Ethernet 100Мбит/с

В 1995 году комитет IEEE 802.3 принял стандарт IEEE 802.3u (дополнительные главы к стандарту IEEE 802.3), описывающий 100-мегабитную технологию Fast Ethernet. Новый стандарт не затронул канальный уровень (подуровни MAC и LLC), соответственно полностью сохранился метод доступа CSMA/CD, форматы кадров и временные соотношения. Все отличия между Ethernet и Fast Ethernet сосредоточены на физическом уровне.

Поскольку одной из целей разработки было обеспечение максимальной преемственности и согласованности 10-мегабитных и 100-мегабитных сетей, было принято решение увеличить скорость за счет сокращения до 10 нс битового интервала (против 100 нс в Ethernet). При этом максимально допустимое время оборота сигнала составило 2,6 мкс, поэтому максимальный диаметр сегмента Fast Ethernet составляет 205 м.

Сети Fast Ethernet могут строиться на волоконно-оптическом (многомодовом) кабеле (два волокна), витой паре 5 категории (две пары) или витой паре 3 категории (четыре пары). Коаксиальный кабель не используется. Сеть всегда строится на концентраторах (или коммутаторах) и имеет иерархическую топологию. Без концентратора можно соединить (при помощи специального кросс-кабеля) только два узла.

Физический уровень делится на подуровень согласования (Reconciliation Sublayer) и устройство физического уровня (Physical Layer Device), связанные через интерфейс, независимый от среды передачи (Media Independent Interface, MII).

Уровень согласования необходим для того, чтобы канальный уровень (точнее, подуровень MAC), рассчитанный на интерфейс AUI, мог работать через интерфейс MII.

Устройство физического уровня выполняет логическое кодирование (4В/5В или 8В/6Т), физическое кодирование (NRZI или MLT-3) и присоединение к среде передачи, а также автоматическое согласование режимов передачи (например, дуплексный или полудуплексный режим).

Версия физического уровня 100BaseFX определяет работу по многомодовому оптоволокну на длине волны 1300 нм. По одному волокну передаются данные от узла, по второму – к узлу. Из FDDI заимствован метод логического кодирования 4В/5В и метод физического кодирования NRZI. В полудуплексном режиме максимальное расстояние между узлами – 412 м, при полном дуплексе – 2 км (по одномодовому оптоволокну – до 32 км). 100BaseFX несовместим с 10BaseFL, поскольку использует другую длину волны.

Версия физического уровня 100BaseTX определяет работу по витой паре (UTP Cat 5 или STP Type 1). Используется две пары, назначение проводников (разводка по контактам разъемов) полностью совпадает с 10-мегабитным Ethernet. Максимальная длина сегмента – 100 м. Логическое кодирование – 4В/5В, физическое кодирование – MLT-3.

Версия физического уровня 100BaseT4 определяет работу по более распространенной и дешевой витой паре (UTP Cat 3). Используется четыре пары: по трем парам передаются данные, четвертая используется для прослушивания несущей частоты и обнаружения коллизий. Логическое кодирование – 8В/6Т, которое обладает более узким спектром сигнала и при скорости 33,3 Мбит/с укладывается в полосу 16МГц (витая пара, 3 категория). Поскольку передача идет одновременно по трем парам, суммарная скорость составляет 100Мбит/с. Максимальная длина сегмента – 100 м.

Устройства, поддерживающие 100BaseTX или 100BaseT4, должны иметь функцию согласования режимов (auto-negotiation), позволяющую выбрать самый эффективный режим, доступный обоим участникам обмена. Всего определено 5 режимов (перечислены в порядке возрастания приоритета): 10BaseT, дуплексный 10BaseT, 100BaseTX, 100BaseT4, дуплексный 100BaseTX.

Для согласования узлы передают пакеты из 17-ти импульсов FLP (Fast Link Pulse), в которых содержится слово, кодирующее наиболее приоритетный из доступных режимов работы. Если один из узлов посылает импульсы NLP (используемые в 10BaseT для контроля целостности линии), второй узел понимает, что единственный возможный режим – это 10BaseT.

Существует еще несколько малораспространенных версий Fast Ethernet, из которых представляет интерес 100BaseSX, работающая по многомодовому оптоволокну на длине волны 830 нм (максимальная длина кабельного сегмента –

300 м). Этот стандарт совместим с 10BaseFL и поддерживает автоматического согласование скорости передачи 10/100 Мбит/с.

В зависимости от того, какой набор методов логического кодирования поддерживает повторитель, он относится к классу I (поддерживает и 4В/5В, и 8В/6Т) или к классу II (поддерживает только один из методов). Повторители класса I порты всех трех типов – 100baseFX, 100BaseTх, 100BaseT4, но, за счет необходимости преобразования схем кодирования, вносят большую задержку – до 140 bt. Поэтому в одном домене коллизий может быть не более одного повторителя класса I. Повторители класса II имеют либо порты 100BaseFX и 100BaseTX, либо только порты 100BaseT4. Вносимая задержка может достигать 92 bt (TX/FX) или 67 bt (t4). Максимальное количество повторителей класса II в одном домене коллизий – 2. Поскольку максимальный диаметр домена коллизий Fast Ethernet для витой пары – 205 м, а каждая станция может быть удалена от повторителя на расстояние до 100 м, в худшем случае повторители (только класса II) должны соединяться кабелем длиной не более 5 м.

10.2. Технология Gigabit Ethernet 1000 Мбит/с

Технология Gigabit Ethernet описывается двумя стандартами: IEEE 802.3z (1998 год) и IEEE 802.3ab (1999 год). Разработчики стандартов старались максимально сохранить идеи классического Ethernet. Как и при переходе от Ethernet к Fast Ethernet, основное новшество состояло в десятикратном (по сравнению с Fast Ethernet) уменьшении длительности битового интервала – до 1нс. Для того, чтобы сохранить максимальный диаметр домена коллизий на уровне 200м, пришлось увеличить минимальный размер кадра с 64 до 512 байт (4096 bt). Если передается короткий кадр, его поле данных должно быть дополнено до требуемой длины запрещенными символами. С другой стороны, эти ограничения диктуются необходимостью распознавания коллизий, что существенно только для полудуплексного режима работы. Для Gigabit Ethernet более характерен дуплексный режим, при котором длина кабельного сегмента ограничивается не временем двойного оборота, а затуханием сигнала и частотными свойствами линии.

Для снижения накладных расходов при передаче коротких кадров (например, подтверждений приема пакетов), предусмотрен пакетный режим передачи (Burst Mode). Узел может передать подряд несколько небольших кадров (не дополняя каждый из них до 512 байт), суммарной длиной не более 8192 байт. Отдельные кадры в такой группе могут быть адресованы разным получателям.

Стандарт IEEE 802.3z определяет следующие версии: 1000BaseSX, 1000BaseLX, 1000BaseCX.

Версия 1000BaseSX определяет работу по многомодовому оптоволокну на длине волны 850 нм. Максимальная длина сегмента при работе в полудуплексном режиме составляет 100 м. В дуплексном режиме максимальная длина кабеля зависит от его полосы пропускания и может достигать 800 м.

Версия 1000BaseLX определяет работу по многомодовому или одномодовому оптоволокну на длине волны 1310 нм. Максимальная длина сегмента для одномодового волокна достигает 5 км, а для многомодового – 550 м.

Версия 1000BaseCX использует в качестве среды передачи твинксильный (twinaxial) кабель, представляющий собой два коаксиальных кабеля (волновое сопротивление 75 Ом) в общей оплетке. По такому кабелю можно организовать только полудуплексный режим. Максимальная длина сегмента составляет 25 м, поэтому такой кабель наиболее применим для связи оборудования в пределах одной комнаты.

Стандарт IEEE 802.3ab определяет версию Gigabit Ethernet на витой паре 5 категории - 1000BaseT. Сигнал физически кодируется с использованием 5 уровней потенциала (код PAM-5) и передается одновременно по четырем парам. Код PAM-5 на тактовой частоте 125 МГц укладывается в полосу пропускания 100 МГц кабеля 5 категории. Для дуплексного режима передача ведется одновременно в обоих направлениях, а для выделения принимаемого сигнала, приемник вычитает из принятой смеси сигналов свой собственный сигнал. Для выполнения этой операции используются цифровые сигнальные процессоры.

10.3. Технология 100VG-AnyLAN

Комитет IEEE 802.12 в 1995 году принял технологии 100VG-AnyLAN, использующую новый метод доступа Demand Priority (приоритет запросов) и поддерживает кадры двух форматов – Ethernet и Token Ring. Эта технология была разработана фирмами Hewlett-Packard и AT&T. Аббревиатура VG (Voice Grade, для голоса) указывает на применимость технологии для телефонии, а AnyLAN (любая ЛВС) означает возможность работы с Ethernet и Token Ring.

Метод доступа Demand Priority основан на централизованном арбитраже доступа к среде передачи. Концентратор циклически опрашивает узлы, подключенные к его портам. Если узел желает передать кадр, он сообщает об этом концентратору и указывает приоритет кадра (всего определено два приоритета - низкий и высокий). Пока сеть занята, запрос ставится концентратором в очередь, обслуживаемую в порядке поступления запросов, но с учетом приоритетов. Если к порту подключен другой концентратор, то концентратор верхнего уровня ожидает, пока он не закончит опрос своих портов. Если сеть свободна, концентратор разрешает передачу пакета, анализирует адрес получателя, и передает кадр только на тот порт, к которому подключен получатель. Фактически, концентратор 100VG-AnyLAN выполняет функции моста: он ведет таблицу MAC-адресов и соответствующих им портов. MAC-адреса узлов определяются в момент их подключения. В отличие от моста, концентратор 100VG-AnyLAN не выполняет буферизацию кадров, а побитно транслирует их в нужный порт.

Первоначальный вариант технологии 100VG-AnyLAN подразумевал использование 4 витых пар категории 3 (и выше). Позже были разработаны версии 100VGF-AnyLAN, работающие по двум парам категории 5 или по многомодовому оптоволокну.

При работе по витой паре 3 категории (гарантированная полоса пропускания 16 МГц), технология 100VG-AnyLAN задействует четыре пары для полудуплексной передачи (дуплексный режим не поддерживается). При этом по каждой паре передается 25 Мбит/с. Логическое кодирование – 5В/6В, физическое – NRZ.

Используется только строго иерархическая топология, допускается наличие до пяти уровней концентраторов. Длина любого кабельного сегмента (узел-концентратор или концентратор-концентратор) при использовании витой пары категории 3 - не более 100 м, а категории 5 – до 200 м. Диаметр сети может достигать 2 км. Максимальное количество узлов в сети – до 1024 (рекомендуется – до 250).

Технология 100VG-AnyLAN не определяет своего формата кадра, а может использовать либо кадры Ethernet 802.3, либо кадры Token Ring 802.5, но в одной сети может использоваться только один тип кадра. Оборудование 100VG-AnyLAN физически несовместимо с оборудованием других технологий, однако выпускались адаптеры 100VG-AnyLAN со встроенной поддержкой Ethernet (и двумя отдельными разъемами для подключения к сети 100VG-AnyLAN и к сети Ethernet). Такие адаптеры позволяли более плавно перейти от Ethernet к 100VG-AnyLAN, заменив сначала адаптеры, и только потом концентратор.

Централизованное управление доступом и наличие системы приоритетов позволяет использовать 100VG-AnyLAN для приложений, чувствительных ко времени отклика – мультимедийных приложений, видеоконференций и т.п.

Технология 100VG-AnyLAN не выдержала конкуренции с более простым и преобладающим (по отношению к Ethernet) стандартом Fast Ethernet, и в настоящее время не развивается.

11. СЕТЕВОЕ ОБОРУДОВАНИЕ ЛОКАЛЬНЫХ СЕТЕЙ

11.1. Сетевые адаптеры

Сетевой адаптер (с драйвером) реализуют физический уровень и подуровень MAC канального уровня. Основная функция сетевого адаптера – передача и прием кадров между компьютером и средой передачи (кабелем).

Передача кадра в кабель состоит из следующих этапов:

- прием через интерфейс LLC-кадра и адресной информации (через общие области памяти)
- оформление MAC-кадра (отброс флагов, заполнение адресов, вычисление CRC)
- логическое кодирование (при использовании избыточных кодов – 4В/5В, 8В/6Т, др.) – если есть необходимость
- выдача сигнала в кабель с использованием физического кода (манчестерский, NRZI, MLT-3, др.)

Прием кадра из кабеля:

- прием сигналов

- выделение сигнала из шума (выделение битовой последовательности)
- логическое декодирование (если оно используется)
- проверка CRC; если ошибка, то кадр отбрасывается, иначе извлекается LLC-кадр и передается LLC-подуровню (через общую область памяти)

Рабочие станции обычно оснащаются более простыми адаптерами, основную работу при этом выполняет драйвер. Для серверов разрабатываются более интеллектуальные адаптеры, со встроенными процессорами и т.п.

11.2. Концентраторы

Основная функция концентратора – повторение каждого полученного сигнала на всех (для Ethernet) или на некоторых портах. Соответственно, наиболее общее название для такого рода устройств – повторитель (repeater). Для 10BaseT Ethernet с топологией “звезда” традиционно используется термин “хаб” (hub). Все эти термины равноправны и взаимозаменяемы. Концентратор работает на физическом уровне модели OSI (поскольку имеет дело с электрическими сигналами, их уровнями, полярностями и т.д.) и на канальном уровне (повторители Ethernet, например, умеют распознавать коллизии), но не выполняет никакого анализа кадров.

К каждому порту концентратора подключаются либо конечные узлы, либо другие концентраторы или другие сетевые устройства, либо (например, в 10Base2 Ethernet) целые физические сегменты кабеля.

Концентратор используется, прежде всего, для увеличения диаметра сети и количества подключенных узлов. Основные технологии локальных сетей допускают использование несколько концентраторов в одной сети, но при некоторых условиях. Например, между любой парой узлов в сети Ethernet может быть не более четырех повторителей (соответственно, максимальный путь включает пять сегментов, причем узлы могут подключаться только к трем из них – так называемое правило “5-4-3”), задержка распространения сигнала между любой парой узлов не должна превышать 25 мкс.

Сеть, построенная на концентраторах, образует единый домен коллизий. Каждый пакет, выданный любой узлом, должен достичь всех остальных узлов, и в это время никакой другой узел не может передавать данные.

С увеличением количества узлов в сети растет частота коллизий, и полезная пропускная способность быстро уменьшается. Для технологий Ethernet приемлемой оказывается нагрузка в 40-50% от максимальной пропускной способности. То есть, пока общий объем передаваемых данных не превышает 40-50% от 10 Мбит/с (для Ethernet), сеть работает нормально, а при росте нагрузки полезная пропускная способность быстро падает. Приемлемое количество узлов в сети, если передаются не мультимедийные данные, лежит около 30.

Конструктивно концентраторы выпускаются в одном из трех вариантов: автономные (standalone), стековые, модульные, модульно-стековые.

Автономные и стековые концентраторы выполняются в виде отдельного корпуса с фиксированным количеством и типом портов (обычно до 24). Все порты, как правило, поддерживают одну среду передачи. Иногда выделяется

порт для подключения к магистрали или каскадирования. Стековый концентратор, кроме того, имеет специальный порт для объединения нескольких таких концентраторов в единое устройство – стек концентраторов. Как правило, в стеке участвует до 8 концентраторов (иногда больше). Модульный концентратор состоит из общего шасси и подключаемых к нему модулей. Разные модули могут иметь разное количество портов и поддерживать разные типы физической среды. Как правило, подключение и отключение модуля не требует выключения концентратора. Обычно модульные концентраторы снабжаются дополнительным модулем SNMP-управления, резервными источниками питания и устройствами вентиляции. Модульно-стековые концентраторы представляют собой модульные концентраторы на небольшое количество модулей с дополнительным портом для соединения их в стек.

Концентраторы могут иметь несколько внутренних шин, образуя несколько разделяемых сегментов. Разные порты концентратора связываются (как правило, не аппаратно, а с помощью программного управления) с разными сегментами. Сами сегменты никак друг с другом не связываются. Такой концентратор называется многосегментным, его способность программно назначать принадлежность портов к сегментам называется **конфигурационной коммутацией** (configuration switching). Когда необходимо соединить эти сегменты, применяют мосты, коммутаторы или маршрутизаторы. Развитием многосегментных концентраторов стали коммутирующие концентраторы, имеющие внутренний мост, связывающий сегменты.

11.3. Мосты

Сеть с единственным доменом коллизий может эффективно работать только при малом количестве узлов. Если необходимо построить сеть среднего или большого размера (десятки, сотни, тысячи узлов), то можно ее разделить на несколько логических сегментов и соединить их устройствами, анализирующими, как минимум MAC-адреса получателей пакетов.

К таким устройствам относятся мосты (bridge), коммутаторы (switch) и маршрутизаторы (router).

Различаются **мосты с маршрутизацией от источника** (source-routing bridge) и **прозрачные мосты** (transparent bridge). Мосты с маршрутизацией от источника характерны для маркерных сетей (Token Ring) и выполняют передачу кадров между сегментами на основании информации о маршруте, предоставленной отправителем кадра. Такие мосты имеют локальные адреса во всех сегментах, к которым они подключены, другие узлы знают об их существовании и целенаправленно взаимодействуют с ними.

Более распространены прозрачные мосты, алгоритм работы которых определен стандартом IEEE 802.1d. Такой мост невидим для других узлов и не имеет своего локального адреса. Мост прослушивает все сегменты, подключенные к его портам, принимает все кадры (запоминая их в буферной памяти), и составляет таблицу MAC-адресов узлов, находящихся в этих сегментах (в эту таблицу попадают пары: номер порта – адрес отправителя). Если адрес получа-

теля принятого кадра неизвестен мосту, то этот кадр передается во все порты, кроме того, откуда он поступил. Так же мост поступает с широковещательными и многоадресными кадрами. Если адрес получателя известен, и получатель подключен к тому же сегменту, из которого пришел этот кадр, то кадр отбрасывается (фильтруется). Фильтрация позволяет изолировать внутрисегментный трафик: кадр, отправитель и получатель которого находятся в одном сегменте, будет отфильтрован мостом и не попадет в другие сегменты. Если адрес получателя известен и относится к другому сегменту, мост передает (транслирует, продвигает - forward) этот кадр в соответствующий порт. Механизм продвижения, как и фильтрация, изолирует трафик: кадр увидят станции только того сегмента, в котором находится получатель.

Производительность моста характеризуется скоростью фильтрации и скоростью продвижения пакетов (обе характеристики измеряются в пакетах в секунду). Мост не транслирует испорченные кадры и кадры, отсеченные коллизией (целостность кадра проверяется вычислением контрольной суммы). Процесс трансляции кадра выполняется мостом в соответствии с методом доступа, например, для Ethernet-сегментов выполняются шаги, предписанные CSMA/CD.

Поскольку узлы могут переноситься из одного сегмента в другой, мосты должны уметь обновлять таблицу MAC-адресов. Обычно это реализуется при помощи ограничения срока годности записи, по истечении которого она удаляется из таблицы. Администратор может пометить часть записей как “статические”, тогда срок годности у этих записей никогда не истечет.

Иногда мосты обладают способностью интеллектуальной фильтрации кадров в зависимости от их содержимого – адресов отправителя и получателя, протокола верхнего уровня, значений некоторых байтов из поля данных кадра.

Мосты работают на подуровне управления доступом к среде передачи (MAC) канального уровня модели ВОС.

11.4. Коммутаторы

Коммутатор (switch) функционально представляет собой высокоскоростной многопортовый мост, способный одновременно связывать несколько узлов на максимальной скорости, обеспечиваемой средой передачи. Часто коммутаторы используются для сегментации – уменьшения размеров доменов коллизий. Фактически, коллизии преобразуются в очереди кадров внутри коммутатора. Предельный случай сегментации – микросегментация – достигается при подключении к каждому порту коммутатора единственного узла, тогда домен коллизий состоит только из узла и порта коммутатора (дуплексный режим позволяет вообще исключить коллизии при микросегментации).

Коммутаторы работают в одном из трех режимов:

1. Коммутация с буферизацией (store-and-forward): каждый кадр целиком записывается в буферной памяти коммутатора, затем проверяется его контрольная сумма, определяется порт назначения, ожидается освобождение порта, и производится передача кадра. Этот способ гарантирует фильтрацию ошибочных и отсеченных коллизией кадров. Основной недостаток – большая задержка передачи, достигающая нескольких миллисекунд на кадр.
2. Коммутация “на лету” (cut-through): кадр передается в порт назначения сразу после приема адреса получателя (в Ethernet – первые 6 байт заголовка кадра). Если в этот момент порт назначения занят, коммутатор обрабатывает пакет в режиме с буферизацией. Коммутация на лету вносит минимально возможную задержку – 11.2 мкс для Ethernet, однако при этом передаются все кадры – в том числе и ошибочные.
3. Бесфрагментная коммутация (fragment-free): коммутатор буферизует первые 64 байта кадра, и, если кадр не длиннее 64 байт, то коммутатор обрабатывает его в режиме с буферизацией. Если кадр длинный, то он передается в порт назначения, как в режиме “на лету”.

Большинство коммутаторов низшего и среднего уровня реализуют только режим коммутации с буферизацией. Коммутация “на лету” характерна для магистральных высокоскоростных коммутаторов, где минимальная задержка передачи гораздо важнее распространения кадров с ошибками. Коммутаторы верхнего уровня иногда используют технологию адаптивной коммутации: сначала все порты работают в режиме “на лету”, затем порты, через которые приходит много кадров с ошибками переводятся в бесфрагментный режим, а если это не помогает отфильтровать ошибочные кадры (в случае длинных пакетов с ошибками), то такие порты переводятся в режим коммутации с буферизацией.

Для достижения высокой производительности (необходимой для одновременного обслуживания всех портов) каждый порт коммутатора, как правило, снабжается отдельным процессором, обычно представляющим собой специализированную микросхему (ASIC), оптимизированную для выполнения функций коммутации. Центральный узел, связывающий процессоры отдельных портов, строится на основе одной из трех схем (применяются и комбинированные варианты):

- коммутационная матрица,

- разделяемая многовходовая память,
- общая шина.

Коммутационная матрица представляет собой комбинационную схему, состоящую, например, из управляемых переключателей, в зависимости от заданного номера порта назначения, соединяющих свой вход с одним из своих выходов. Таким образом, коммутационная матрица физически коммутирует каналы связи между портами, обеспечивая наиболее быстрый способ связи процессоров портов. Основным недостатком коммутационной матрицы – ограниченное число портов в таких коммутаторах (сложность схемы матрицы возрастает пропорционально квадрату числа портов). Кроме того, при использовании коммутационной матрицы необходимо, чтобы каждый порт мог самостоятельно буферизовать входящие кадры, иначе, за время возможного ожидания освобождения выходного порта, кадры могут быть потеряны.

Разделяемая многовходовая память позволяет увеличивать количество портов коммутатора без усложнения его схемы. Процессоры портов для передачи данных друг другу используют общую память. Переключение входа и выхода памяти осуществляет специальный блок управления, который организует по очереди данные для каждого выходного порта. По запросу входного порта блок управления подключает его к входу требуемой очереди, а процессор порта записывает в нее данные кадра. При появлении полных кадров в очередях, блок управления поочередно подключает выходные порты к своим очередям для считывания кадров для передачи.

Процессоры портов в коммутаторах с общей шиной снабжаются, с одной стороны, модулями арбитража доступа к шине, а с другой стороны – фильтрами, отбирающими передающиеся по шине ячейки, предназначенные данному порту. Кадр в таких коммутаторах передается по шине не целиком, а небольшими частями – ячейками, что позволяет (вместе с высокой скоростью передачи данных по шине) реализовать псевдопараллельный режим передачи кадров между портами. Для работы без блокировок пропускная способность общей шины должна быть не меньше половины суммы пропускных способностей всех портов.

Сложные коммутаторы, как правило, комбинируют приведенные архитектуры. Например, для модульных концентраторов свойственно использование общей шины для соединения модулей, в то время, как внутри каждого модуля (обычно не более 12 портов) реализуется наиболее быстрая архитектура – коммутационная матрица.

В зависимости от варианта конструкции, различают:

- автономные (standalone) коммутаторы,
- стековые коммутаторы,
- модульные коммутаторы на основе шасси.

Первые два варианта имеют фиксированное число (обычно 8,16,24, редко до 30) и тип портов, которые не могут быть изменены. Автономные коммутаторы применяются на уровне рабочих групп. Стековые коммутаторы отличаются от автономных наличием дополнительного (стекового) интерфейса, позволяющего объединять несколько таких коммутаторов в систему, работающую, как

единый коммутатор – стек коммутаторов. Как правило, количество коммутаторов в стеке не превышает четырех (пропускная способность стекового интерфейса лежит в пределах 200-400 Мбит/с).

Стековые коммутаторы применяются в сетях, где емкости автономного коммутатора уже недостаточно (количество узлов больше 30), а установка значительно более дорогого модульного коммутатора неоправданна. Модульные коммутаторы на основе шасси позволяют подключать необходимое количество разнотипных модулей, часто с возможностью их замены без выключения коммутатора (hot swap). Количество портов в таких коммутаторах может превышать 100. Как правило, модульные коммутаторы используются в качестве магистральных.

В сетях Ethernet/Fast Ethernet часто используется сетевое устройство промежуточного типа – коммутирующий концентратор (switching hub), представляющий собой двухсегментный концентратор (один сегмент – Ethernet, другой – Fast Ethernet), сегменты которого соединены двухпортовым мостом. В результате все Ethernet-станции, подключенные к нему, образуют один домен коллизий, а все Fast Ethernet-станции – второй домен коллизий. Соединения же между станциями разных сегментов обслуживаются мостом. Такие устройства, как правило, дешевле, чем полноценные коммутаторы. Наиболее эффективно они используются при наличии большинства Ethernet-станций и высокоскоростном (Fast Ethernet) подключении одного-двух серверов. Поскольку все высокоскоростные узлы образуют один домен коллизий, то при увеличении их количества производительность сети будет падать.

11.5. Алгоритм покрывающего дерева

Алгоритм покрывающего дерева (Spanning Tree Algorithm, STA) описан в стандарте IEEE 802.1D и позволяет ликвидировать петли в сети (если в сети есть кольцевые маршруты, это может привести к неправильной работе мостов и коммутаторов). Алгоритм STA из всех связей, имеющих в сети, выбирает подмножество, образующее дерево, покрывающее все узлы сети. Алгоритм STA состоит из четырех этапов.

4. В сети выбирается корневой коммутатор (root switch), который будет считаться корнем дерева. Выбор происходит либо автоматически (корневым становится коммутатор с наименьшим значением MAC-адреса блока управления), либо выполняется администратором.
5. Для каждого коммутатора определяется корневой порт (root port) – порт, через который проходит самый короткий путь до корневого коммутатора.
6. Для каждого сегмента сети выбирается назначенный порт (designated port) – порт, через который проходит кратчайший путь от данного сегмента до корневого коммутатора.
7. Все порты, не вошедшие в корневые и назначенные, блокируются.

При определении кратчайших расстояний рассчитывается суммарное время (в 10-наносекундных единицах) передачи одного бита данных от выбранного порта до корневого коммутатора (учитывается только времена пере-

дач по связям между коммутаторами). Например, для Ethernet-сегмента время передачи равно 10, а для Fast Ethernet – 1.

Все коммутаторы периодически обмениваются служебными пакетами – протокольными блоками данных моста (Bridge Protocol Data Unit, BPDU), содержащими идентификатор корневого коммутатора, расстояние до корня, идентификатор коммутатора, выдавшего этот пакет, идентификатор порта, на который был выдан пакет и еще несколько служебных полей. После включения каждый коммутатор считает себя корневым (если иное не задано администратором) и выдает пакеты BPDU со своим идентификатором в поле “идентификатор корневого коммутатора” и расстоянием до корня, равным 0, через все свои порты. Если коммутатор получает BPDU, в котором идентификатор корневого коммутатора меньше его собственного идентификатора, он перестает генерировать свои пакеты, а ретранслирует приходящие пакеты нового корневого коммутатора, увеличивая в них поле “расстояние до корня” на условное время сегмента, по которому пришел этот пакет. При этом коммутатор запоминает для каждого порта минимальное расстояние до корня (из всех пришедших на этот порт пакетов BPDU).

Через заданное время процесс конфигурации заканчивается и корневым портом коммутатор считает тот свой порт, у которого расстояние до корня оказалось минимальным (если таких портов несколько, выбирается порт с наименьшим идентификатором). Затем, он делает назначенными все порты, принятые по которым минимальные расстояния до корня больше, чем расстояние до корня корневого порта. Наконец, все порты, кроме корневого и назначенных, переводятся в заблокированное состояние.

В процессе дальнейшей работы корневой коммутатор продолжает генерировать пакеты BPDU, а остальные коммутаторы продолжают их ретранслировать. Если за установленное время тайм-аута корневой порт какого-либо коммутатора не получает BPDU, он инициирует новую процедуру построения покрывающего дерева.

СПИСОК ЛИТЕРАТУРЫ

1. **Компьютерные сети. Принципы, технологии, протоколы.** / В.Г.Олифер, Н.А.Олифер. — СПб: Издательство “Питер”, 1999. — 672 с.: ил.
2. **Высокопроизводительные сети. Энциклопедия пользователя:** Пер. с англ./Марк А. Спортак и др. — К.: Издательство “ДиаСофт”, 1998. — 432с.
3. Кульгин М. **Технологии корпоративных сетей. Энциклопедия** — СПб: Издательство “Питер”, 2000. — 704 с.: ил.
4. Гук М. **Аппаратные средства локальных сетей. Энциклопедия** – СПб.: Издательство “Питер”, 2000. –576с.:ил.
5. **Компьютерные сети+.** Учебный курс (MSCE 70-058)/Пер. с англ. — М.: “Русская редакция”, 2000. — 552с.
6. **Сети Windows NT 4.0:** Пер. с англ. /Джон Д. Рули и др. — К.: Издательская группа ВHV, 1997. — 800с.
7. Мельников Д.А. **Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели...** – М: КУДИЦ-ОБРАЗ, 1999. – 256с., ил.
8. Якубайтис Э.А. **Информационные сети и системы.** Справочная книга. — М.: Финансы и статистика, 1996. — 368с.: ил.
9. Ратынский М.В. **Основы сотовой связи** / Под ред. Д.Б. Зимина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2000. – 248с.:ил.
10. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. **Структурированные кабельные системы**, 3-е изд. – М.: “Компьютер-Пресс”, 2001. – 608с.

ИНТЕРНЕТ

1. Русские документы: сетевые технологии <http://www.rusdoc.ru/net.shtml>
2. Сетевые протоколы <http://www.protocols.ru>
3. Аналитический обзор базовых стандартов СКС http://www.ecolan.ru/st_review.htm
4. Техническая библиотека компании BiLiM Systems <http://www.bilim.com>
5. Сервер информационных технологий: сетевые технологии <http://www.citforum.ru/nets/>
6. Книги по сетям <http://document.newmail.ru/la.htm>
7. Термины и основные понятия телекоммуникаций <http://www.online.ru/it/helpdesk/race/index.htm>
8. Архив: проектирование сетей <http://www.osp.interline.ru/archive/35.htm>
9. Практика проектирования сетей <http://kgg.moldline.net/>

Учебное издание

Брейман Александр Давидович

Сети ЭВМ и телекоммуникации. Учебное пособие.
Часть 1. Общие принципы построения сетей. Локальные сети.
