Министерство образования и науки Российской Федерации

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

ФАКУЛЬТЕТ ДИСТАНЦИОННОГО ОБУЧЕНИЯ (ФДО)

А. В. Пуговкин

СЕТИ ПЕРЕДАЧИ ДАННЫХ

Учебное пособие

Томск
2015

УДК 004.7(075.8)
ББК 32.973.202я73
П 880

Рецензенты:
Богомолов С. И., канд. техн. наук, доцент кафедры телекоммуникаций и основ радиотехники ТУСУРа;
Бацула А. П., канд. техн. наук, советник генерального директора научно-производственной фирмы «Микран».

Пуговкин А. В.

П 880 Сети передачи данных : учебное пособие / А. В. Пуговкин. — Томск : факультет дистанционного обучения ТУСУРа, 2015. — 138 с.

Рассмотрены основные вопросы построения и функционирования сетей передачи дискретных сообщений (компьютерных сетей), технология передачи и коммутации пакетов, даны материалы по локальным вычислительным сетям Ethernet, по межсетевому взаимодействию (протоколы TCP/IP, PPP), сетям доступа, включая радиодоступ и волоконно-оптические сети, по интеграции служб и услуг.

Для студентов очной и заочной форм обучения, а также студентов, обучающихся с применением дистанционных образовательных технологий, изучающих дисциплины «Системы и сети передачи дискретных сообщений», «Сети ЭВМ и телекоммуникации» и др.

УДК 004.7(075.8)
ББК 32.973.202я73

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Компьютерные сети или сети передачи дискретных сообщений — такой же атрибут современного общества, как и авиация, автомобильный транспорт, банковская система и т. п. [1–3]. Они позволяют не только общаться своим абонентам, но и получать разнообразную информацию, совершать сделки, выполнять финансовые операции, проводить дистанционное обучение и многое, многое другое.

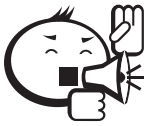
Начало развитию компьютерных сетей было положено в 60-е годы, когда к мощным компьютерам стали подключать несколько удаленных абонентских терминальных устройств, расположенных как в одном здании, так и на больших расстояниях. Здесь для соединения использовались либо местные коаксиальные линии, либо телефонная сеть и модемы. С появлением мини-ЭВМ и персональных компьютеров в 70-е — 80-е годы их стали объединять для совместной работы. Тогда появились и утвердились такие технологии локальных сетей, как Ethernet, Token Ring и др.

Вместе с локальными сетями развивались и сети глобального масштаба. Совершенствование телекоммуникаций от аналоговых систем связи на многоканальных электрических кабелях до цифровых систем передачи и распределения на волоконно-оптических линиях породило быстрое внедрение конкуренции и сменяемость технологий глобальных сетей. Созданная для низкоскоростных ненадежных телефонных сетей технология X.25 сменилась технологией Frame Relay, а та, в свою очередь, так и не успев стать массовой, уступила место целому созвездию: IP, Gigabit Ethernet, ATM, которые не только жестко конкурируют, но и дополняют друг друга.

Классификацию компьютерных сетей (сетей передачи данных — СПД) можно проводить по различным признакам. Наиболее распространено деление сетей по территориальному признаку:

1. Локальные вычислительные сети (ЛВС) — сети масштаба предприятия, покрывающие небольшую территорию размером не более 2–3 км.
2. Региональные сети, покрывающие территорию города или области.
3. Глобальные вычислительные сети (ГВС) — сети масштаба государства или мировые сети.

Компьютерные сети можно различать по типу применяемой технологии: IP, ATM, NGN, однако возможность инкапсуляции и конвертации протоколов позволяет строить многопротокольные сети.



Основным технологическим отличием СПД от телефонных сетей является применение способа коммутации пакетов.

Суть его заключается в следующем. Сообщение сначала преобразуется в цифровую форму, а потом разбивается на части (пакеты). Каждый пакет может передаваться самостоятельно, поскольку в его составе содержится адресная информация пункта назначения. Рисунок 1 иллюстрирует один из способов коммутации пакетов (дейтаграммный). Здесь пакеты с номерами 1, 2, 3, 4 поступают на узел коммутации *A*, который определяет оптимальный (кратчайший) путь *ACDB* и отправляет по нему пакет 1. При поступлении пакета 2 ситуация в сети изменилась, путь *ACDB* не обеспечивает быстрого прохождения, и узел *A* отправляет пакет 2 по другому пути (*AFDB*). К моменту окончания пакета 2 ситуация в сети восстанавливается, и пакеты 3, 4 снова идут по пути *ACDB*. Может получиться так, что к узлу *B* пакеты придут не в той последовательности, в которой были отправлены. Узел *B* восстанавливает порядок следования пакетов.

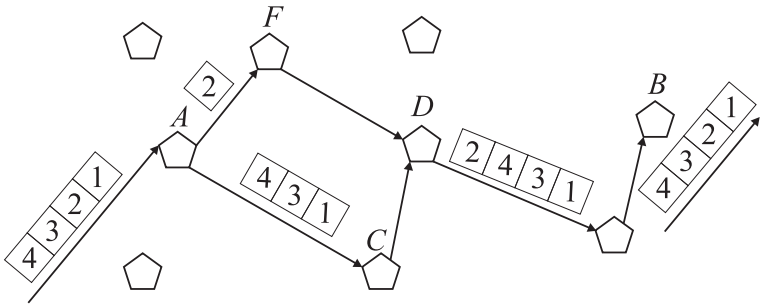


Рис. 1 – Коммутация пакетов

Основные процедуры при передаче пакетов:

- разбиение сообщения на пакеты;
- запись пакетов в узлах;
- маршрутизация пакетов в соседние свободные узлы.

Достоинства технологии коммутации пакетов:

- высокая загрузка канала (до 100%) обеспечивается тем, что любые паузы в сообщении одного абонента могут быть заполнены пакетами информации других абонентов;
- возможность многоадресной передачи, так как в заголовке пакета может содержаться разное количество адресов.

Недостатки способа коммутации пакетов:

- перезапись информации в узлах, что увеличивает задержку передаваемых сигналов;

- переменная скорость передачи и переменная задержка, что также связано с буферизацией информации, ограниченным объемом памяти запоминающих устройств и с возможностью различных путей распространения информации.

На рисунке 2 приведена типичная структура пакета. Он ограничен с двух сторон флагами. Чаще всего это комбинация из восьми бит (например, 011111110). Адресное поле содержит информацию об адресах отправителя и получателя. В поле управления указывается тип пакета, его размер и формат, указания по обработке сигнала и т. п.

флаг	адрес	управление	информация	контрольное поле	флаг

Рис. 2 – Структура пакета

В информационном поле передаются непосредственно данные, а контрольное поле предназначено для процедуры обнаружения ошибок посредством передачи определенных кодовых комбинаций, которые проверяются на приемном конце.

Метод коммутации пакетов обеспечивает высокую надежность передачи информации и высокую степень загрузки канала. Это предопределило его широкое применение как для передачи данных, так и в системах передачи речи и сигнализации. IP-телефония — это пример пакетной передачи речи, а ОКС-7 — современная система сигнализации, использующая технологию коммутации пакетов. Сети следующего поколения NGN (Next Generation Networks) также используют принцип коммутации пакетов.

В качестве примера того, что нам предстоит изучать, рассмотрим сеть передачи данных масштаба области (рис. 3).

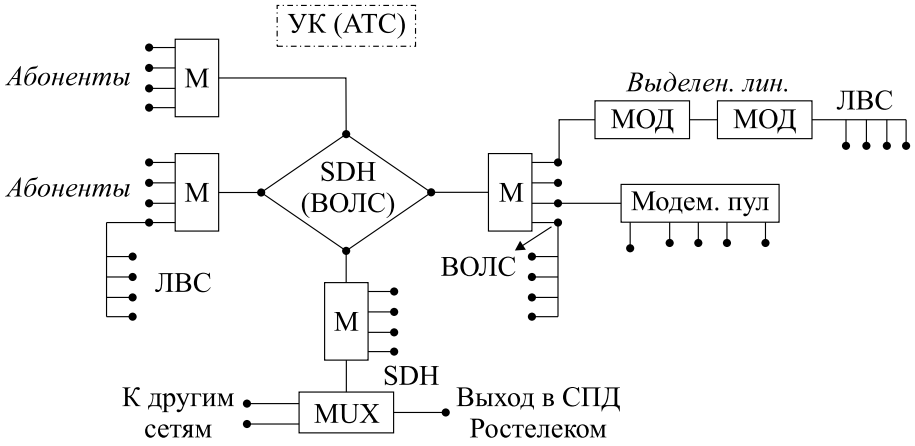


Рис. 3 – СПД масштаба области: М — маршрутизатор; УК — узел коммутации; МОД — модем; MUX — мультиплексор

Здесь опорная сеть синхронной цифровой иерархии SDH на основе одномодовой волоконно-оптической линии связи (ВОЛС) и узлов коммутации (АТС) предоставляет свои услуги СПД, т. е. сеть передачи данных является наложенной. Мультиплексоры ввода-вывода, входящие в состав УК, одним из своих портов подключены к маршрутизаторам, которые и обеспечивают коммутацию пакетов по

IP-технологии. К другим портам маршрутизаторов подключены абоненты: ЛВС, модемные пулы, абоненты «on line», работающие в режиме постоянного подключения по выделенной линии. Эти подключения возможны как по ВОЛС, так и по медным кабелям с помощью модемов.

Один из узлов маршрутизации обеспечивает связь с сетью России, а также с другими операторами и с районами области.

Соглашения, принятые в книге

Для улучшения восприятия материала в данной книге используются пиктограммы и специальное выделение важной информации.

Этот блок означает внимание. Здесь выделена важная информация, требующая акцента на ней. Автор здесь может поделиться с читателем опытом, чтобы помочь избежать некоторых ошибок.

Контрольные вопросы по главе

Глава 1

ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕЙ

1.1 Основные определения

Начальным этапом изучения является формулирование некоторых основных определений.

Сеть передачи данных — выделенная или наложенная система телекоммуникаций, которая через узлы маршрутизации (коммутации) и сеть доступа позволяет абонентам обмениваться различной информацией, представленной в цифровой форме в виде последовательного набора фрагментов сообщения (пакетов). Другое определение сети является более узким и направлено только на вычислительные способности распределенных систем.

Компьютерная сеть — система распределенной обработки информации, состоящая из территориально разнесенных компьютеров, взаимодействующих между собой с помощью средств связи.

Есть и другие определения сетей, но мы будем пользоваться первым, более общим, так как в его основе лежит именно телекоммуникационная составляющая, не зависящая от прикладных процессов.

Сеть доступа — набор технических и программных средств (мультиплексоры, модемы, линии связи, протоколы и др.), обеспечивающих абонентам выход в СПД.

Узел коммутации, или *сетевой узел*, — элемент сети, где происходит перераспределение потоков данных по различным направлениям. При этом не конкретизируется, на базе каких протоколов и аппаратных средств (хаб, коммутатор, маршрутизатор и т. п.) это реализуется.

Маршрутизатор (узел маршрутизации), *router* — узел, управляющий пересылкой данных по сети с использованием системы адресов третьего сетевого уровня семиуровневой эталонной модели взаимодействия открытых систем (ЭМВОС).

Протокол — набор правил для одной из коммутационных функций. Например, PPP (Point to Point Protocol) — протокол для организации канала передачи данных в режиме «точка-точка», а IP (Internet Protocol) — набор правил для маршрутизации данных.

Стек протоколов — набор организованных по уровням ЭМВОС протоколов, которые, работая совместно, позволяют прикладным процессам обмениваться данными. Например, стеком протоколов являются PPP, IP, TCP.

Пакет, или *элемент данных протокола*, — передающийся по сети форматированный элемент данных, который включает в себя полезную и служебную информацию.

Хост — компьютер, который выполняет как приложения, так и сетевые функции и является конечной точкой сети. Как персональные компьютеры, так и мини-ЭВМ и большие ЭВМ попадают под определение хоста.

1.2 Взаимодействие компьютеров. Топологии сетей

Самым простым вариантом является связь двух компьютеров. Это взаимодействие может быть организовано различными способами, в зависимости от выбранной технологии на первом и втором уровнях ЭМВОС [1, 4]. Наиболее распространенные в настоящее время варианты приведены на рисунке 1.1.

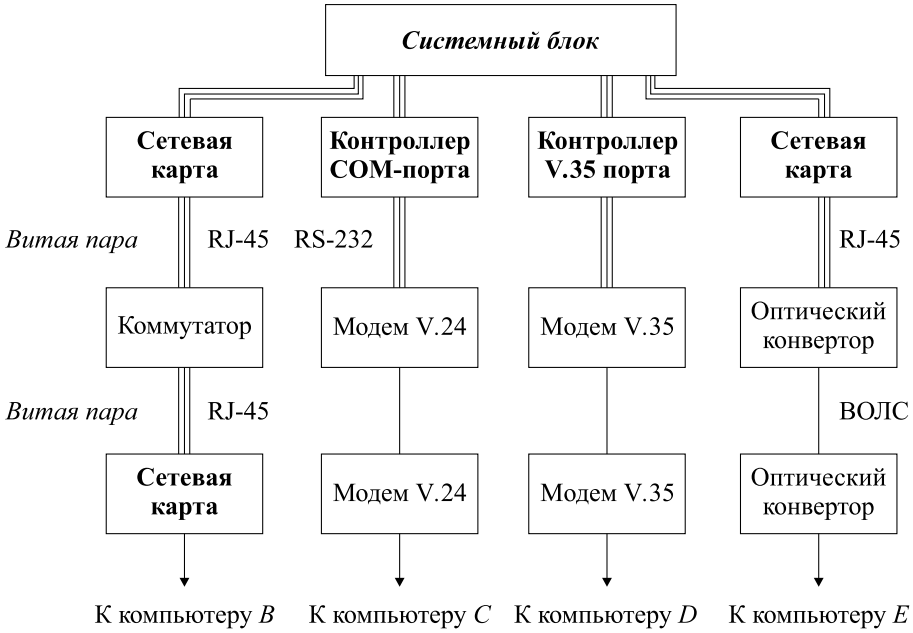


Рис. 1.1 – Варианты взаимодействия компьютеров

Системный блок компьютера передает данные другому компьютеру сначала по многоразрядным параллельным шинам к контроллерам, обеспечивающим передачу в линии связи. Такими контроллерами могут быть контроллер COM-порта с интерфейсом RS-232C, контроллер на основе протокола V.35, сетевая карта Ethernet с выходным портом RJ-45. Каждый из этих контроллеров организует свой режим передачи:

- сетевая карта — полудуплексный или дуплексный Ethernet по витой паре или волоконно-оптической линии связи;
- COM-порт и порт RS-232C — соединение по коммутируемой линии (dial up) с помощью модемов серии V.24 и т. п.;
- интерфейс V.35 с помощью соответствующих модемов и выделенной линии — постоянное соединение в синхронном или асинхронном режиме передачи.

Эти варианты соединения двух компьютеров являются основой для создания сетей, когда число взаимодействующих хостов больше и значительно много больше двух. Способ организации физических или логических связей компьютеров называется *топологией сети*.

Рассмотрим основные топологии (рис. 1.2).

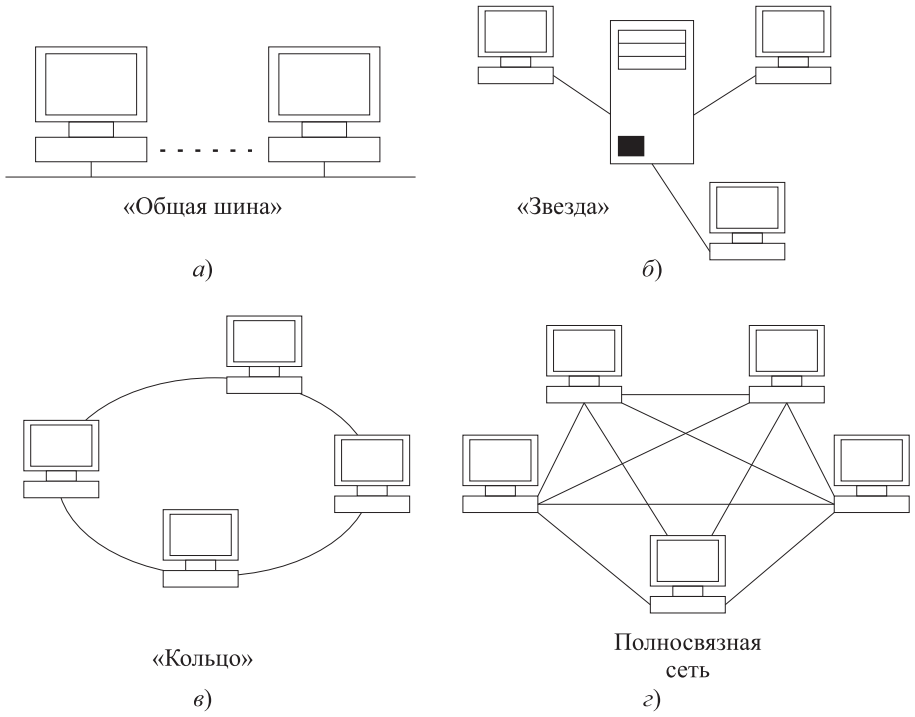


Рис. 1.2 – Основные топологии компьютерных сетей: *а*) шина; *б*) звезда; *в*) кольцо; *г*) комбинированная

Топология «шина» — одна из первых, когда к общей линии на некотором расстоянии друг от друга подключены компьютеры. Поскольку между ними нет никакой развязки, в определенный момент времени осуществлять передачу данных может только один абонент, который выходит на передачу, убедившись, что линия свободна. Все остальные прослушивают линию, дожидаясь, когда она освободится. Такой режим передачи и приема является полудуплексным, и он может сопровождаться конфликтами (коллизиями), когда на режим передачи одновременно выходит несколько абонентов. Такой метод доступа абонентов к сети носит название «Множественный доступ с контролем несущей и обнаружением коллизий» — МДКН/ОК.

В топологии «шина» отсутствует ведущий узел сети — все абоненты равноправны, а добавление новых абонентов до поры до времени осуществляется довольно

просто. Здесь не страшны повреждения отдельных станций, все остальные при этом продолжают работать в нормальном режиме.

Топология «шина» помимо ситуации с коллизиями имеет и другие существенные недостатки. Так, в центральной линии при подключении к ней компьютеров возникают неоднородности, от которых отражаются электромагнитные волны, что приводит к появлению ложных сигналов, интерференция падающих и отраженных волн создает в линии большие неравномерности по уровню сигнала. К таким же эффектам приводит и несогласование центральной линии на ее концах и короткое замыкание в любой точке.

Размер сети не может быть большим по двум основным причинам:

1. Затухание сигнала в физической линии.
2. Конечная скорость распространения волны в линии приводит к тому, что информация о возникшем конфликте не успевает дойти до станции, отправившей пакет, и она начинает передавать следующий пакет, в то время как предыдущий оказался испорченным.

Топология «звезда» может быть реализована в двух вариантах: пассивная и активная. Пассивная звезда в центре имеет многопортовый повторитель (концентратор, хаб), который любой пакет, приходящий на один из своих портов, ретранслирует на все остальные порты. Поэтому по своим сетевым возможностям пассивная звезда ничем не отличается от «шины».

В центре активной звезды стоит коммутатор, который наделен функциями управления: дает разрешение на передачу, осуществляет адресное соединение и т. д.

В ***топологии «кольцо»***, как правило, используют два кабеля между узлами: на передачу и на прием. Все узлы равноправны и обладают свойствами регенератора, это позволяет строить довольно протяженные сети. Кольцевая топология обладает высокой надежностью и устойчивостью к перегрузкам. При разрыве кольца (повреждение кабеля или узла) пакеты могут быть направлены в обратном направлении (в «обход»).

1.3 Взаимодействие компьютеров. Адресация

При объединении компьютеров в сети возникает задача их идентификации. Она решается с помощью системы адресов.

Требования к адресу следующие:

1. Уникальность в мировой системе.
2. Иерархичность структуры адресов.
3. Компактность записи.
4. Удобство для пользователя при опознавании адреса.
5. Минимизация труда администратора при составлении адресных таблиц. Крайне необходимо, чтобы этот процесс шел автоматически.

Удовлетворить всем этим требованиям с помощью одной системы адресации невозможно, поэтому в настоящее время используют сразу три системы:

1. Аппаратные адреса — уникальные цифровые адреса сетевых карт, которые задаются их производителями. Эти адреса функционируют на канальном уровне

ЭМВОС и непосредственно могут работать только в небольших локальных сетях. Для адресации в больших сетях они не применяются, так как не обладают свойством иерархичности. Поэтому таблицы, составляемые из таких адресов, очень громоздки и сложны для администраторов сетей.

2. Числовые (сетевые) адреса — это тоже уникальные цифровые адреса, но они присваиваются не сетевым картам, а пользователям единой международной организацией IANA — Internet Assigned Numbers Authority — комиссией по константам Интернет. Система регистрации описана в документе RFC2050, а деятельность IANA — в RFC1700. В этой системе задается номер сетевого узла в старших битах и номер хоста в младших битах. Например, адрес класса С в IP-сетях задается так (табл. 1.1).

Таблица 1.1 – Пример задания адреса класса С

Номер узла			Номер хоста
11000100	00001011	11111111	00000001

Или в сокращенной (десятичной записи)

196	11	255	1

Такая система записи сравнительно компактна (32 бита), имеет постоянный размер, а главное — иерархична.

3. Цифровые адреса при всех своих достоинствах неудобны для пользователей. Их неудобно запоминать и трудно идентифицировать с конкретными объектами. Поэтому в сетях передачи данных также используются символьные адреса или имена. Например, tor.rk.tusur.ru или www.panasonic-batteries.com.

Недостатками таких адресов являются переменный формат, большая длина и отсутствие глобальной иерархичности.

Использование всех трех систем адресации осуществляется следующим образом. Пользователь задает символьный адрес. Компьютер переводит его в числовой (сетевой) адрес. При взаимодействии пакета с сетевой картой в ЛВС используется аппаратный адрес. Такая система представляется громоздкой, но зато позволяет абоненту работать как в локальных, так и в глобальных сетях.

1.4 Организация каналов передачи

Взаимодействие компьютеров предполагает установление между ними канала передачи. С точки зрения семиуровневой модели взаимодействия открытых систем эта процедура реализуется на физическом и канальном уровнях. В состав канала передачи (рис. 1.3) входят:

- оконечное оборудование данных (ООД) или DTE (Date Terminal Equipment) — это терминальное оборудование (компьютер, маршрутизатор);
- аппаратура передачи данных (АПД) или DCE (Date Circuit Terminating Equipment), которая связывает компьютеры или ЛВС с линиями связи. Примеры АПД — модемы, порты мультиплексоров, сетевые карты компьютеров. Оборудование АПД работает на физическом уровне;

- линия связи обеспечивает непосредственную передачу сигнала по каналу. Физической средой в линиях связи является волоконно-оптический кабель, многопарный электрический кабель, коаксиальный кабель, радиолинии;
- между двумя хостами в канале передачи на большие расстояния есть узлы связи (коммутаторы, мультиплексоры ввода-вывода, маршрутизаторы). Их функция заключается в организации канала передачи (сетевой уровень) и пропускании пакетов при организованном канале.

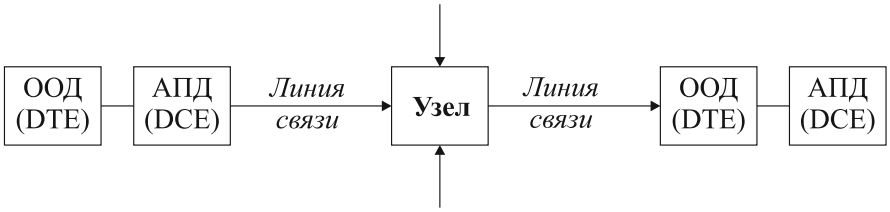


Рис. 1.3 – Канал передачи

Вопросы, связанные с физической средой передачи, модемами, цифровыми системами передачи и распределения рассмотрены в смежных дисциплинах («Основы построения телекоммуникационных систем и сетей», «Сети связи и системы коммутации» и др.). Поэтому в этом разделе будут рассмотрены только особенности построения и работы каналов передачи применительно к компьютерным сетям.

В компьютерных сетях применяют физическое кодирование и логическое кодирование. Физическое кодирование в терминологии цифровых систем передачи выполняет функции линейного кодирования (синхронизация, минимизация ширины спектра, высокая энергетическая эффективность). Наиболее распространенными являются коды: потенциальные (NRZ, AMI, 2B1Q) и импульсные (биимпульсный, манчестерский). Некоторые из этих кодов будут рассмотрены подробней при описании конкретных сетей.

Логическое кодирование предназначено для улучшения характеристик линейных кодов, для обнаружения и исправления ошибок, для шифрования данных. При логическом кодировании указанные последовательности «нулей» и «единиц» заменяются специальными кодовыми последовательностями. Примерами таких кодов являются HDB-3, 4B5B, 4B3T и др. Некоторые из этих кодов будут рассмотрены ниже.

Синхронизация в сетях передачи данных, так же как и в цифровых системах передачи, подразделяется на побитовую (тактовую) и кадровую (цикловую). Побитовая синхронизация реализуется путем выделения тактовой частоты, а кадровая — применением специальных синхробайтов (рис. 1.4, *а*).

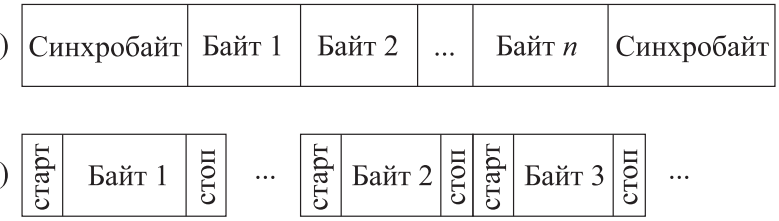


Рис. 1.4 – Синхронная (*а*) и асинхронная (*б*) передачи

В этом случае для *n* байт используется один или несколько синхробайтов. Код синхробайта может быть разным, например 01111110 или 01010101. Такой метод передачи называется синхронным.

Для линий с низким качеством применяют асинхронный режим передачи (рис. 1.4, *б*). Здесь каждый байт обрамляется битами «старт» и «стоп», и тогда он может передаваться независимо от других. Между байтами допускаются временные задержки переменной величины. Метод асинхронной передачи проще и дешевле. Однако он требует большего удельного веса служебных бит и работает на сравнительно низких скоростях (до 115 Кбит/с).

Метод синхронной передачи имеет большее быстродействие, но он сложнее в реализации. Поэтому синхронные модемы дороже асинхронных.

1.5 Структуризация и объединение сетей

Если сеть содержит небольшое количество станций с небольшими расстояниями между ними, то они физически связаны одной из простейших топологий (шина, звезда, кольцо, полносвязная). Такая сеть называется однородной. С увеличением числа станций ($n > 20$) и расстояния между ними проявляется влияние затухания сигналов и уменьшение скорости передачи вследствие коллизий. Для устранения этих недостатков большие сети разбивают на отдельные однородные сегменты, между которыми помещаются активные устройства, регенерирующие сигнал с целью усиления и восстановления формы, а также ограничивающие взаимный трафик. Эта процедура носит название структуризации сети. При этом предполагается, что все сегменты сети работают в одном стеке протоколов (например, Ethernet-IP).

В качестве активных устройств, разделяющих сети на сегменты, используются концентраторы (хабы), коммутаторы или маршрутизаторы.

1. Структурированная сеть на хабах приведена на рисунке 1.5.

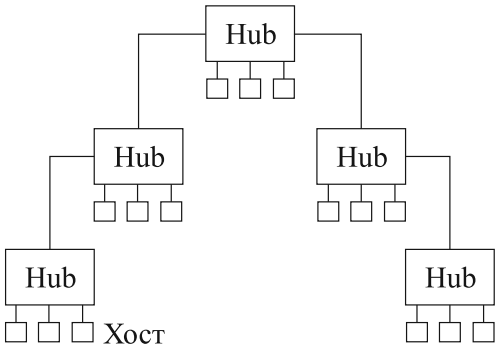


Рис. 1.5 – Сеть на хабах

Порт каждого хаба ретранслирует поступающие пакеты на выходы всех остальных своих портов. Поэтому в конечном итоге на всех портах всех хабов появляется один и тот же пакет. Таким способом решается проблема компенсации затухания и искажения формы импульса, но остается проблема коллизий и создания излишней нагрузки на станции, которые получают все пакеты, а не те, которые им предназначены. Можно сказать, что хабы обеспечивают физическую структуризацию сети,

но не обеспечивают логической структуризации, так как информационные потоки не упорядочились.

2. Структурированная сеть на коммутаторах имеет ту же структуру, что изображена на рисунке 1.5, только вместо хабов включены коммутаторы. Коммутаторы — это многопортовые устройства, они могут анализировать аппаратные адреса получателей и путем внутренних переключений направлять пакеты только на один из выходных портов. На все другие порты пакеты не передаются. Если к порту коммутатора подключена ЛВС на хабах, то весь внутренний трафик будет замыкаться внутри этой ЛВС, а внешний (предназначенный станциям других сегментов) передаваться на другие порты. Про такую схему можно сказать, что в ней есть и физическая, и логическая структуризация.

3. Структурированная сеть на маршрутизаторах — *R* (router) приведена на рисунке 1.6.

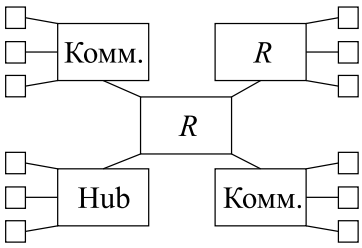
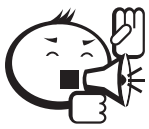


Рис. 1.6 – Схема на маршрутизаторах

Здесь маршрутизатор, так же как и коммутатор, селектирует пакеты, но не с помощью аппаратных адресов, а по сетевым адресам получателя. Изоляция трафика в сегментах более надежна, масштаб сети значительно больше (не только локальные, но и глобальные сети).



Можно сказать, что названные выше активные устройства служат объединению сетей. Это действительно так, если рассматривать сети, работающие по одним протоколам. Если же нам надо связать станции, относящиеся к сетям с различными протоколами, например X.25 и IP, то обычных коммутаторов и маршрутизаторов недостаточно. В этом случае применяют специальные шлюзы, которые осуществляют переход от одного протокола в другой. Один из способов реализации шлюза — метод инкапсуляции (рис. 1.7), когда пакет одного протокола, например IP, в шлюзе снабжается заголовком протокола X.25.

Теперь IP-пакет может проходить по сети с другим протоколом. Основные проблемы реализации такого шлюза:

- шлюз должен работать как на передачу, так и на прием;
- добавление заголовка снижает скорость передачи;

- усложнение системы адресации. Поскольку взаимодействующие сети имеют разные системы адресации, в шлюзе должны быть таблицы перехода от одних адресов к другим. Составление таких таблиц совершается вручную;
- для реализации шлюза нужны специализированные устройства — пограничные маршрутизаторы.

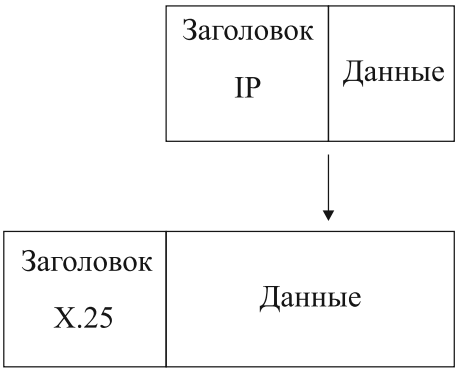


Рис. 1.7 – Инкапсуляция протоколов

Контрольные вопросы по главе 1

1. Дайте понятие и приведите примеры стека протоколов сети передачи данных.
2. Перечислите достоинства и недостатки топологий «звезда» и «шина».
3. Какие интерфейсы используются в каналах связи?
4. Назовите иерархичные системы адресации.
5. Назовите узловые элементы, обеспечивающие структуризацию сетей.

Глава 2

ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ (ЛВС)

2.1 Общие понятия

Локальная вычислительная сеть (ЛВС) — это коммуникационная система, поддерживающая в пределах здания или группы зданий один или несколько высокоскоростных каналов передачи цифровой информации, подключенных к устройствам (ЭВМ) кратковременно [1, 3, 6, 7, 10].

ЛВС появились в связи с развитием элементной базы РЭА, а также благодаря усовершенствованиям архитектуры и технологии производства ЭВМ. На некотором этапе закон Гроша (производительность ЭВМ равна квадрату его стоимости), который был справедлив для первых суперкомпьютеров, перестал действовать. Другими словами, суперкомпьютеры перестали удовлетворять пользователей как по скорости обработки информации, так и по удобству обращения с ними. Появилась необходимость осуществления взаимодействия ЭВМ: разделение вычислительных и информационных ресурсов. Первые разработки в области ЛВС появились в начале 70-х годов, а пик их развития пришелся на середину/конец 80-х. Новое дыхание технике ЛВС придали технологии коммутации (начало 90-х) и более высокоскоростные версии ЛВС (Fast Ethernet, Gigabit Ethernet, 10 Gb Ethernet).

В настоящее время ЛВС применяются для объединения ЭВМ в различных масштабах: от рабочих групп до сетей предприятия и кампусных сетей. Таким образом, локальные сети позволяют строить масштабируемые сети в узком смысле этого слова. Локальные сети обеспечивают взаимодействие ЭВМ, что необходимо для работы распределенных приложений обеспечения электронного документооборота, исследовательских сетей с параллельными вычислениями, групп разработчиков и т. д.

При разработке ЛВС предполагалось, что наиболее важным аспектом этих сетей будет стоимость аппаратуры и линий связи, поэтому в качестве среды взаимодействия многих станций используется некий общий разделяемый ресурс, который

используется всеми станциями совместно в режиме разделения времени (TDMA). Данные требования привели к использованию следующих типов топологий:

- шина (bus);
- кольцо (ring);
- звезда (star).

По методу доступа различают сети:

- со случайным (стохастическим) доступом (Ethernet);
- пропорциональным (маркерным) доступом (Token Ring).

Метод доступа к среде обуславливает характеристики того или иного типа ЛВС: нагрузочная способность, прогнозируемость задержек и т. д. Функционирование происходит на двух нижних уровнях модели ЭМВОС (рис. 2.1): физическом и канальном.

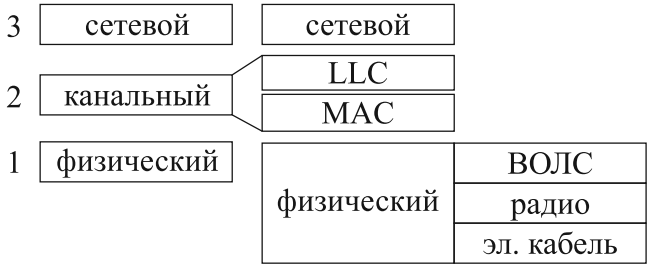
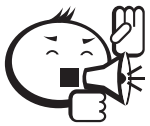


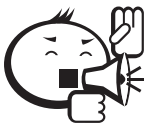
Рис. 2.1 – Структура уровней



Спецификации на ЛВС определяют разделение канального уровня на два подуровня:

- управления доступом к среде (Media Access Control) — MAC. Функция доступа к каналу и арбитража (CSMA/CD). Здесь одной из главных функций является адресация;
- управления логическим звеном канала данных (Logical Link Control) — LLC. Функции соединения абонентов и контроля потока пакетов. Этот подуровень определяет механизмы взаимодействия с протоколами верхних уровней (сетевого). Практически все распространенные семейства протоколов сетевого и более верхних уровней осуществляют поддержку ЛВС.

Спецификации физического уровня для ЛВС разнообразны и включают в себя практически все известные физические среды: от простого телефонного кабеля до оптоволокна, включая коаксиал и радиоканалы, что позволяет передавать данные с высокими скоростями.



Адресация в ЛВС подразумевает использование типичных для сетевых окружений адресов (MAC-адресов):

- индивидуальный адрес (unicast) — обеспечивает однозначную идентификацию каждого устройства на канальном уровне;
- групповой адрес (multicast) — обеспечивает доставку кадра некоторой группе хостов, взаимодействующих с разделяемой средой;
- широковещательный (broadcast) — обеспечивает доставку кадра всем станциям в данной ЛВС.

Отличительными признаками ЛВС являются:

- высокая скорость передачи (10–1000 Мбит/с);
- низкий уровень ошибок ($P \leqslant 10^{-7}$–10^{-8});
- быстродействующий механизм управления обменом;
- ограниченное число компьютеров, подключенных к сети.

2.2 Управление доступом к сети

Поскольку число абонентов (компьютеры, серверы, принтеры и т. д.) в ЛВС может быть достаточно велико, то им необходимо обеспечить доступ к общим разделяемым ресурсам. Этот доступ может быть как равноправный, так и с приоритетом. Чаще всего используют равноправный случайный доступ. Для этого информация каждого абонента разбивается на пакеты (рис. 2.2).

Преамбула	Адрес получателя	Адрес отправителя	Управление	Данные	Контрольная сумма

Рис. 2.2 – Структура пакета

Длина пакета может быть различной — от нескольких десятков байт до нескольких килобайт. Назначение преамбулы, или стартовой комбинации, — обозначить начало пакета, организовать синхронизацию, настроить сетевую карту получателя на прием и обработку пакета.

Поле управления существует для указания типа пакета (если они разные по содержанию), его номера, размера и формата. Поле контрольной суммы служит для обнаружения и исправления ошибок.

Существует два способа доступа к сети:

1) *детерминированный*, который работает по четким правилам предоставления доступа абонентам. При этом конфликты (коллизии) при доступе нескольких абонентов в сеть исключены. Примером такого способа является маркерный доступ (рис. 2.3). Здесь право доступа передается от узла

к узлу с помощью специального пакета, называемого маркером или токеном. Этот способ реализован в сетях FDDI и Token Ring;

2) *случайный*, когда абоненты получают доступ непредсказуемым образом и поэтому здесь возможны конфликты. Скорость доставки пакетов не контролируется. Она тем меньше, чем больше трафик в сети и чем больше вероятность коллизий. Такой способ реализован в сетях Ethernet и носит название МДКН/ОК или CSMA/CD. Расшифровка этих сокращенных названий следующая:

   - МДКН/ОК — множественный доступ с контролем несущей и обнаружением коллизий;
   - CSMA/CD — Carrier Sense Multiple Access/Collision Detection.

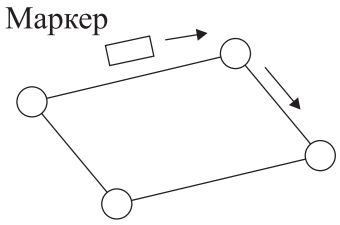


Рис. 2.3 – Маркерный доступ в кольцевой схеме

Рассмотрим суть CSMA/CD. CSMA — рабочие станции (компьютеры) подключены к общей шине. С помощью приемника сетевой карты каждая из них контролирует наличие сигнала в общей шине. При присутствии сигнала какой-либо другой станции пакет данных не передается. Как только передача другой станции закончится, начинается передача собственного пакета. CD — определяет наличие и процедуру устранения коллизий. Если две станции начали передачу одновременно или с небольшим сдвигом во времени, то их пакеты накладываются друг на друга и оба пакета искажаются. Чтобы устранить последствия коллизий, станции прослушивают сеть и после передачи пакета. При обнаружении коллизии станция повторяет передачу через случайный отрезок времени, и так продолжается несколько раз до тех пор, пока пакет не будет передан.

Сеть, работающая по алгоритму CSMA/CD, имеет ограничения на ее размер (диаметр) по двум основным причинам:

1. Затухание сигнала в линиях, соединяющих элементы сети (компьютеры, хабы, коммутаторы).
2. Условие «необнаружения коллизий». Суть этого фактора поясним с помощью рисунка 2.4. Пусть станция Ст. 1 начинает передачу своего пакета. Пока начало этого пакета не дошло до самой удаленной станции N, она может начать передачу своего пакета. Допустим, что эта передача началась непосредственно перед приходом пакета Ст. 1, т. е. через время $\tau_3 = L/V$. Возникла коллизия. Информация об этом дойдет до станции отправителя также через время $\tau_3 = L/V$.

Общая задержка (время двойного оборота) составит $2\tau_3 = 2L/V$. Если за это время пакет станции Ст. 1 не закончится, то Ст. 1 передачу пакета прекращает

и он считается не переданным. Но если пакет закончится, то станция Ст. 1 будет считать его успешно переданным и начнет передавать следующий пакет. Потеря пакета может быть обнаружена только на прикладных (верхних) уровнях, когда пройдет значительное время.

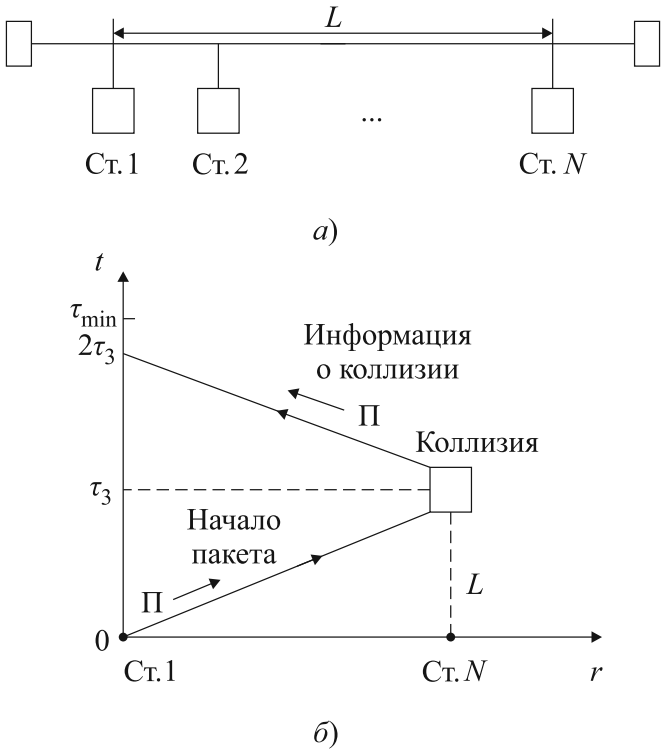


Рис. 2.4 – Влияние коллизий на диаметр сети: *а*) схема; *б*) диаграмма

Таким образом, условие

$$\tau_{min} > 2\tau_3 = 2\frac{L}{V},$$

где τ_{min} — минимальная длительность пакета, накладывает ограничение на диаметр сети; $L < \tau_{min} V/2$.

Развитием технологии Ethernet является режим множественного доступа с контролем несущей и предупреждением коллизий CSMA/CD. Суть этого режима заключается в следующем — в сети выделяется головной (ведущий) узел, остальные узлы — ведомые. Ведомый узел, желающий передать информацию, посылает ведущему пакет запроса. Если сеть свободна, то ведомый узел получает разрешение на передачу информации. Эта технология широко применяется в сетях радиодоступа (IEEE 802.11, IEEE 802.15).

2.3 Принцип распределения адресов

Уникальный адрес присваивается сетевой карте в процессе ее изготовления. Формат адреса содержит 48 бит (рис. 2.5), что позволяет сформировать 280 триллионов различных адресов. Этого с избытком хватит всем производителям сетевых карт.

1 бит	1 бит	22 бита	24 бита
I/G	U/L	OUI-идентификатор	OUA

Рис. 2.5 – Формат MAC-адреса

В формате адреса есть поле идентификатора (OUI), в котором в двоичном коде записывается уникальный номер производителя сетевых карт. Этот номер присваивается международным комитетом IEEE. Максимальное число таких номеров 2^{22} — более четырех миллионов. Вторая часть адреса (OUA) — это непосредственно сетевой адрес карты. Его присваивает производитель сетевой карты. Каждый производитель может изготовить до 16 миллионов сетевых карт с уникальными номерами. Сочетание полей идентификатора и сетевого адреса с большим запасом обеспечивает адресное пространство для всех пользователей земного шара.

Поле I/G отличает индивидуальные номера I — Individual (значение бита равно 0) и групповые G — Group (значение бита равно 1).

Поле U/L (Universal/Local) содержит значение бита, равное 0, для обычной адресации и 1 — для местной, когда адресное поле OUA изменено пользователем.

2.4 Ethernet — базовая технология ЛВС

2.4.1 Общие сведения

Отличительные особенности Ethernet: передача в основной полосе и случайный доступ к среде.

Передача в прямой полосе — прямая (немодулированная) передача данных по сети. Способ передачи, при котором цифровой сигнал направляется непосредственно в канал связи без всякой модуляции (т. е. несущая частота отсутствует по определению). Для уменьшения ширины спектра, а также для улучшения статистических характеристик битовой последовательности используют разные типы линейного кодирования (Манчестер, NRZ, NRZI) и различные типы скремблирования. Данный тип передачи иногда называют «передача с постоянной составляющей».

Доступ к среде: CSMA/CD — протокол асинхронного временного разделения (т. е. полудуплексное функционирование), который был разработан для использования в пакетной спутниковой связи.

Ethernet подразумевает топологию типа «шина», однако это касается только логического функционирования, и зачастую на физическом уровне используется более гибкая звездообразная топология.

2.4.2 Стандарты Ethernet

Общие принципы функционирования Ethernet приведены на рисунке 2.6. В текущий момент времени в сети Ethernet может передавать только одна станция — остальные, прослушивая текущую передачу, ждут ее окончания.

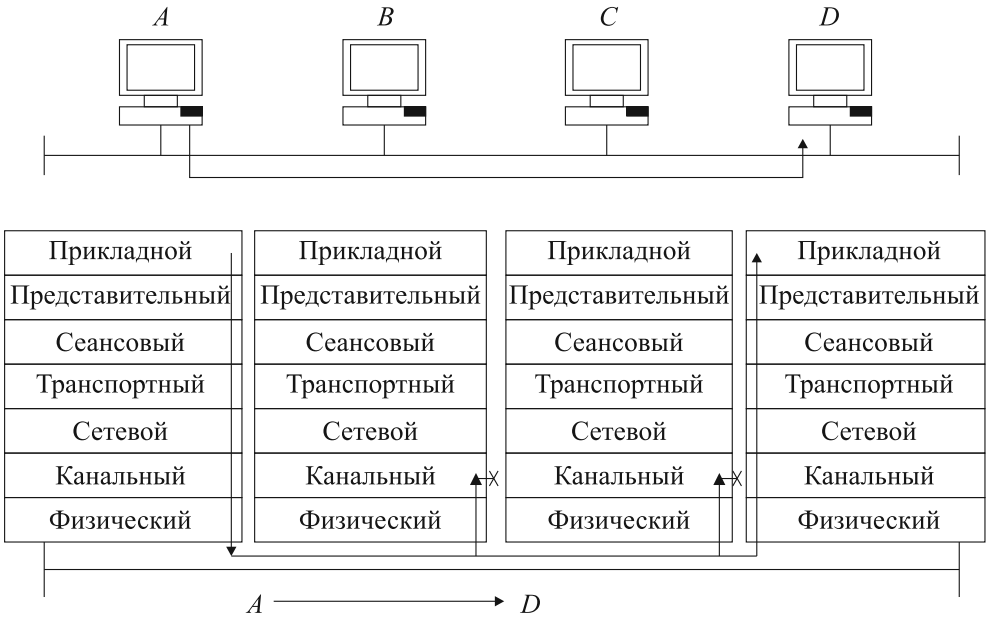


Рис. 2.6 – Функционирование Ethernet

Перед началом передачи станция выдерживает определенный интервал времени, а только затем начинает передавать, одновременно прослушивая среду на предмет возникновения конкурирующей передачи, возникшей одновременно с текущей. Если посторонняя передача обнаружена, то станция прекращает передачу на некоторое случайное время (аналогично поступают и другие станции, притом даже не участвовавшие в данном конфликте), а затем делает попытку повторной передачи. Сети Ethernet обладают очень полезным свойством — широковещательностью, которая очень часто используется протоколами верхних уровней в служебных целях.

Структура стандартов выглядит следующим образом (рис. 2.7).

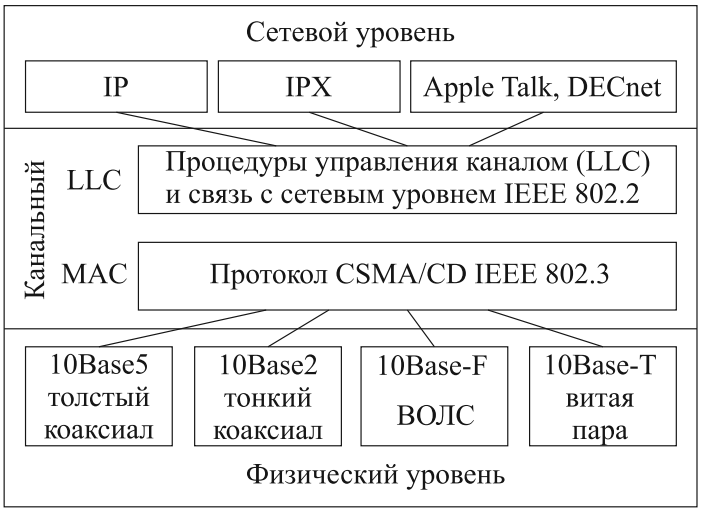


Рис. 2.7 – Структура стандартов IEEE

В этой структуре на физическом уровне отражены как устаревшие технологии, основанные на применении коаксиального кабеля (10Base5, 10Base2), так и со-

временные, использующие витую пару (10Base-T), и волоконно-оптические линии (10Base-F). Технологии с коаксиальным кабелем, использующие топологию «общей шины», помимо применения дорогого кабеля требуют сложных подключений отрезков коаксиальных кабелей к основной коаксиальной шине. Эти подключения создают неоднородности в линии и приводят к появлению в ней отраженных волн, что приводит к неустойчивой работе ЛВС.

Технология 10Base-T сейчас наиболее распространена. В ее основе лежит топология «звезда» (рис. 2.8), где в центре «звезды» размещается многопортовый повторитель, называемый концентратором или хабом. Назначение концентратора заключается в регенерации на всех своих портах сигналов, поступающих от одной из станций. Например, пакет, приходящий от станции *A* на порт 1 через порты 2, 3, 4, ретранслируется по всем остальным станциям.

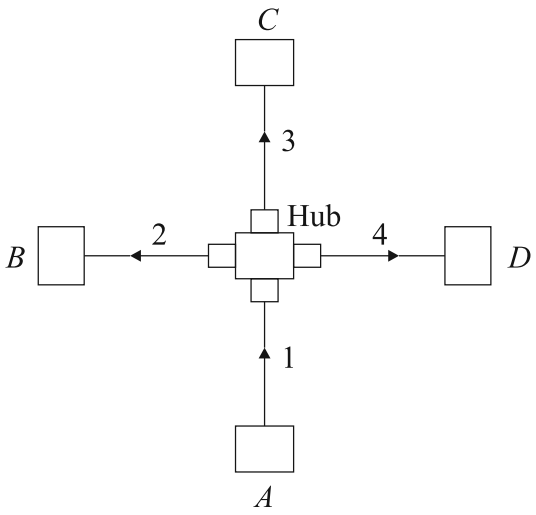


Рис. 2.8 – Топология ЛВС с концентратором

Порты хаба соединяются со станциями с помощью электрического кабеля «витая пара» UTP и разъемов RJ-45 или RJ-11. Максимальное расстояние между хабом и станцией (длина сегмента) $l_{\text{сегм}}$ зависит от типа кабеля и составляет:

$$l_{\text{сегм}} = \begin{cases} 100 \text{ м, UTP-3;} \\ 150 \text{ м, UTP-5.} \end{cases}$$

Основные достоинства стандарта 10Base-T:

- дешевый кабель;
- простота подключения станций.

К недостаткам следует отнести:

- малую длину сегмента вследствие затухания сигнала в линии;
- больший уровень внешних помех по сравнению с коаксиальным вариантом.

Несмотря на различия в физической топологии, логической топологией в 10Base-T остается «общая шина» и все правила CSMA/CD. Технология 10Base-F позволяет увеличить длину сегмента до 2000 м при использовании многомодового (ММ) волоконно-оптического кабеля. Такая среда передачи не чувствительна к электрическим наводкам, обладает высокой помехоустойчивостью.

2.4.3 Способы линейного кодирования в Ethernet

В сетях Ethernet нет отдельных линий связи для передачи сигналов синхронизации между передатчиком и приемником, т. е. синхронизация осуществляется за счет выделения приемником синхросигнала непосредственно из принимаемой битовой последовательности. Такой метод синхронизации носит название «в основной полосе» (in band), и он предъявляет некоторые требования к методу линейного кодирования.

Существуют два альтернативных метода включения тактовой информации в битовый поток.

1. Амплитудный или потенциальный (представление 1/0 разными амплитудами (полярностями)) RZ, NRZ, NRZI (AMI), HDB-3, 2B1Q. Недостатки метода: значительная полоса сигнала, плохие самосинхронизирующие качества (необходимость дополнительных преобразований сигнала), в отдельных ситуациях — сложность реализации кодера/декодера.
2. Фазовый или манчестерский (рис. 2.9). Код разделяет битовый интервал на две половины. Логическая «1» кодируется переходом из низкого уровня к высокому, а логический «0» наоборот. Таким образом, перепад осуществляется при любых передаваемых битах, включая долговременные однотипные последовательности из одних 0 или 1, что определяет хорошие синхронизационные способности данного кода. Битовый интервал — 100 нс.

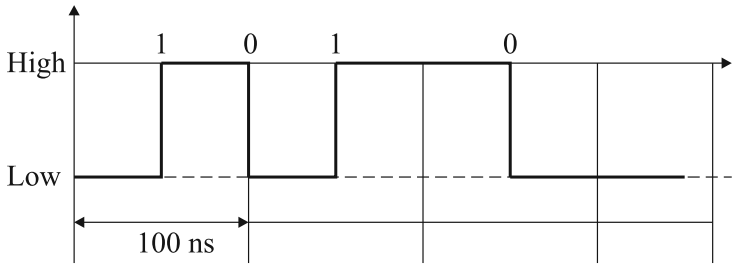


Рис. 2.9 – Манчестерский код

Таким образом, при передаче любого пакета уровень постоянной составляющей практически равен половине амплитуды. В Ethernet используются сигналы отрицательной полярности.

2.4.4 Алгоритм доступа к сети Ethernet

При более подробном описании алгоритма доступа вводятся следующие понятия.

- *IPG (Interpacket Gap)* — минимальное расстояние между пакетами. Для Ethernet — это 9.6 мкс.
- *BT (Bit Time)* — время передачи одного бита (100 нс для Ethernet).
- *PDV (Path Delay Value)* — удвоенное значение времени прохождения сигнала между двумя узлами.
- *Окно коллизий* — максимальное значение PDV для данного сегмента сети.

- *Slot time (время канала)* — максимально допустимое окно коллизий для сегмента (512 BT).

Процедура передачи кадра следующая:

1. При первой попытке прослушивается сеть, и при отсутствии других сигналов начинается передача пакета при соблюдении времени IPG и отсутствии коллизий.
2. Если в процессе передачи возникла коллизия и она обнаружена, то станция, обнаружившая ее, посылает специальный сигнал предупреждения, называемый пробкой. «Пробка» содержит 32 бита. Пакеты, пострадавшие от коллизий, уничтожаются.
3. После некоторой случайной задержки производится следующая попытка передачи пакета. Всего таких попыток — 16. С увеличением номера попытки увеличивается интервал времени ожидания.
4. После шестнадцатой неудачной попытки передача пакета прекращается, и управление от сетевой карты передается компьютеру.
5. Все дальнейшие действия осуществляются под руководством протоколов верхних уровней.

2.4.5 Форматы кадров Ethernet

В сети IEEE 802.3/Ethernet существуют в общей сложности четыре протокольные модификации Ethernet, не сильно отличающиеся друг от друга. Более того, базовых формата кадра всего два — Ethernet II и IEEE 802.3, причем они отличаются назначением всего одного поля (рис. 2.10) Ethernet II/DIX.

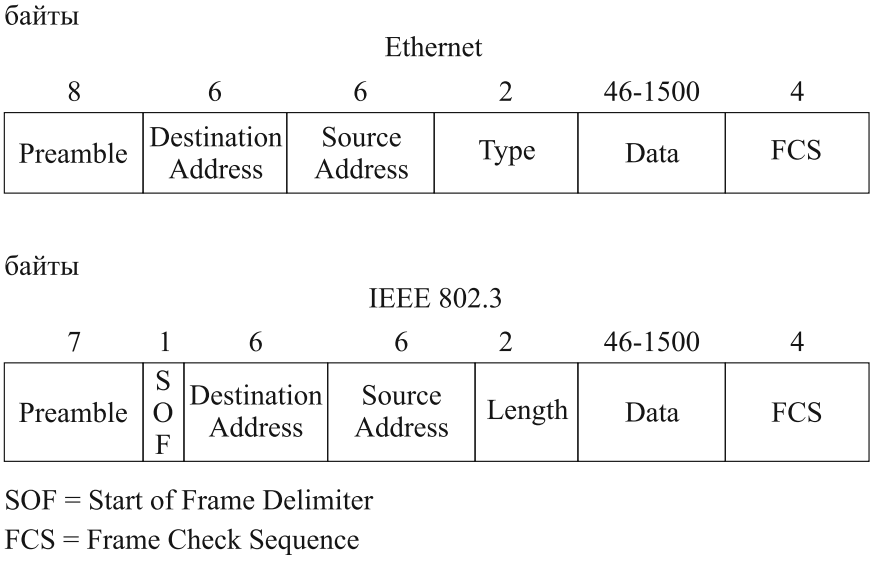


Рис. 2.10 – Базовые форматы кадров Ethernet

Preamble (Преамбула): Стартовая комбинация, состоящая из последовательности чередующихся нулей и единиц. Необходима для настройки аппаратуры адаптера или другого сетевого устройства на прием и обработку пакета, т. е. на оповещение принимающих станций о начале кадра и синхронизацию передающей

и приемных станций. Кроме того, она необходима для надежного выявления коллизий и эффективной борьбы с явлением ложной несущей (Fast Carrier Event, FCE). (Стандарт IEEE 802.3).

SOF/SFD (Start-of-frame Delimiter, Разделитель начала кадра): Двоичная последовательность 10101011, которая служит для разделения преамбулы и следующего за ним поля, а также для окончательной синхронизации приемных станций двумя младшими битами (Стандарт IEEE 802.3). В Ethernet II преамбула не разделяется на собственно преамбулу и начальный ограничитель кадра, что является одним из отличий Ethernet от IEEE 802.3, хотя весьма несущественным. Тем более что очень часто преамбула вообще рассматривается как часть физического механизма синхронизации передающей и принимающей сторон, а не как часть кадра. В физической реализации сетевого адаптера Ethernet преамбула и SFD генерируются специальными логическими схемами непосредственно перед передачей в среду.

Destination Address/Source Address (Адрес Ethernet/MAC-адрес): Состоит из 12 шестнадцатеричных цифр (48 битов/6 байтов). Первые 6 цифр MAC-адреса содержат идентификатор производителя (код поставщика — vendor code), который также называют Organizational Unique Identifier (OUI), назначаемый IEEE. Последние 6 цифр назначаются производителем и часто представляют собой серийный номер. Таким образом, данная структура адреса обеспечивает абсолютную уникальность сетевых устройств.

В подавляющем большинстве сетевых адаптеров MAC-адрес прошит в ПЗУ (его часто называют burned-in address — BIA). При инициализации сетевого устройства этот адрес переписывается в ОЗУ.

Адреса Ethernet могут быть обычными, групповыми и широковещательными. Мультикастные адреса имеют старшую часть «010000». Многоадресная передача принимается всеми станциями, групповой адрес которых совпадает с указанным в поле адресом получателя. Если же все биты адреса равны единице, то это широковещательный адрес (broadcast address), и такой пакет предназначен всем станциям. В Ethernet режим широковещательного обращения реализуется посредством установки в единичное значение всех битов адреса получателя — OFFFFFFFFFFFh.

Одно из небольших отличий между Ethernet и 802.3 состоит в классификации групповых адресов. В отличие от Ethernet спецификация 802.3 подразделяет групповые адреса на адреса, имеющие глобальное и локальное значение. Однако это разделение редко используется на практике.

Length (IEEE 802.3): Поле длины кадра состоит из двух байтов и определяет длину поля данных от поля Length до поля FCS (от 0 до 1500 байтов). Однако ввиду ограничений на минимальную длину кадра поле данных не может быть короче 46 байт. Если же объем передаваемых данных меньше, то поле данных дополняется заполняющими битами.

Type (Ethernet II): Данное поле определяет протокол верхнего уровня, принимающего данные после завершения обработки кадра на канальном уровне. Содержит шестнадцатеричное число, из списка стандартных протоколов (RFC 1700). Для протокола IP — 0800h (RFC 894), для протокола ARP — 0806h (RFC 1700), а для протокола RARP — 8O35h (RFC 1700). По сути это функция подуровня LLC.

Data: Поле содержит инкапсулированные данные верхних уровней, например в случае использования стека протоколов TCP/IP это IP-дейтаграмма. В отличие от служебных полей поле данных имеет переменную длину, причем оно не может

быть короче 46 байт и длиннее 1500 байт. Фактически эта величина является MTU (Maximum Transmission Unit). В случае, когда реальный объем передаваемых данных меньше 46 байт (например, для эмуляции терминала часто передается всего один символ, вводимый с клавиатуры), поле данных дополняется до минимального размера заполнителем. Байт заполнения может вставляться, даже если объем передаваемых данных более 46 байт. По предложению Novell, в случае нечетного количества байт драйвер сетевой платы добавляет еще один. Это сделано потому, что некоторые старые маршрутизаторы не понимают кадры нечетной длины. Ограничения на MTU сверху определены эффективностью работы сети с точки зрения производительности в случае большого числа станций, а снизу — надежным опознаванием коллизий. Таким образом, максимальный размер кадра Ethernet составляет 1526 байт (12 208 бит), а минимальный — 72 байт (576 бит). Как уже отмечалось ранее, очень часто преамбулу и разделитель начала кадра не включают в логическую структуру кадра, т. к. данные поля генерируются на аппаратном уровне вне зависимости от содержимого кадра. Поэтому оперируют несколько другими цифрами минимальной и максимальной длины кадра — 64 байта (512 бит) и 1518 байтов (12 144 бит) соответственно.

При битовой скорости передачи 10 Мбит/с время передачи пакета минимальной длины составляет 57.6 мкс. Это время несколько больше, чем удвоенное время распространения сигнала между крайними точками кабеля, равное 51.2 мкс.

FCS (Frame Check Sequence): Последнее поле в кадре — это четырехбайтное поле контрольной последовательности кадра (Frame Check Sequence, FCS). Значение этого поля вычисляется на основе содержимого заголовка и данных (вместе с заполнителем, но без учета преамбулы и ограничителя) с помощью 32-разрядного циклического избыточного кода (Cyclic Redundancy Code, CRC-32) по стандартной процедуре вычисления остатка от деления двоичного массива данных на порождающий полином вида

$$P(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

и дальнейшего сравнения остатка от деления с полем FCS. В случае несовпадения результата деления и содержимого поля FCS пакет считается испорченным и игнорируется. Данный код позволяет обнаружить 99.999999977% всех ошибок в сообщениях длиной до 64 байтов. Таким образом, вероятность того, что принимающая станция воспримет испорченный кадр как целый, практически равна нулю.

IEEE 802.2 (LLC) Header and Data: В соответствии с эталонной моделью OSI каждый протокольный блок данных содержит (инкапсулирует) пакеты вышележащих протоколов своего стека. Протокол 802.3 описывает метод доступа к среде передачи — нижний подуровень канального уровня, и для него вышележащим протоколом является протокол логического управления каналом (Logical Link Control, LLC) — верхний подуровень канального уровня. Таким образом, согласно требованиям стандарта, поле данных должно содержать заголовок LLC. Однако в ранних версиях NetWare компания Novell проигнорировала этот заголовок и стала помещать пакеты IPX/SPX непосредственно за полем длины кадра, и поле данных начиналось так же, как и обычный заголовок IPX, с двух байтов, состоящих из единиц (число 0×FFFF). Иными словами, Novell использовала кадры просто в качестве

контейнера. В принципе, применение базового формата кадра 802.3 без служебной информации верхнего подуровня канального уровня позволяет Novell несколько сократить накладные расходы в расчете на кадр. Но выигрыш оказался невелик, а в гетерогенной среде применение нестандартного формата привело к проигрышу, так как маршрутизатор или сетевая плата вынуждены проверять дополнительные поля для определения типа пакета. Это послужило одним из побудительных мотивов того, что, начиная с версии 4.0, Novell перешла по умолчанию на стандартный формат Ethernet 802.2. Другой причиной оказалось то, что использование базовых кадров Ethernet 802.3 делало невозможным применение таких опций защиты, как подпись пакетов, из-за фиксированного поля контрольной суммы пакета, равного 0×FFFF, чтобы кадр Ethernet 802.3 можно было отличить от других типов кадров.

Спецификации IEEE предусматривают всего два стандартных формата — 802.2 и 802.2 SNAP, причем второй является естественным расширением первого. Стандартный кадр должен содержать в поле данных служебную информацию логического управления каналом (LLC), а именно: однобайтное поле точки доступа к сервису для получателя (Destination Service Access Point, DSAP), однобайтное поле точки доступа к сервису для отправителя (Source Service Access Point, SSAP) и однобайтное управляющее поле (Control) (см. рис. 2.11). Назначением номеров точек доступа к сервису (Service Access Point, SAP) занимается IEEE, и он выделил следующие номера:

0×E0 для Novell; 0×F0 для NetBIOS;
0×06 для TCP/IP; AA для SNAP.

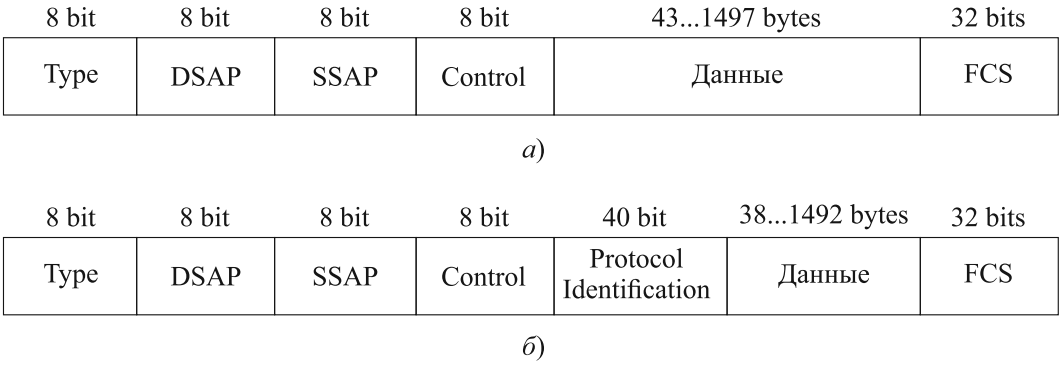


Рис. 2.11 – Фрагменты кадра IEEE 802.3 формата 802.2 (*а*) и 802.2 SNAP (*б*)

Таким образом, поля DSAP и SSAP служат для определения вышележащего протокола и, как правило, содержат одно и то же значение. Структура этих полей показана на рисунке 2.12. В них:

- I/G = 0 — индивидуальный адрес;
- I/G = 1 — групповой адрес;
- C/R = 0 — команда;
- C/R = 1 — подтверждение.

Управляющее поле определяет тип кадра по классификации HDLC (I — информационный, S — супервизорный, U — ненумерованный) и обычно задается равным

0×03 (в соответствии с протоколом LLC это означает, что соединение на канальном уровне не устанавливается, однако осуществляется подтверждение о приеме — LLC3).

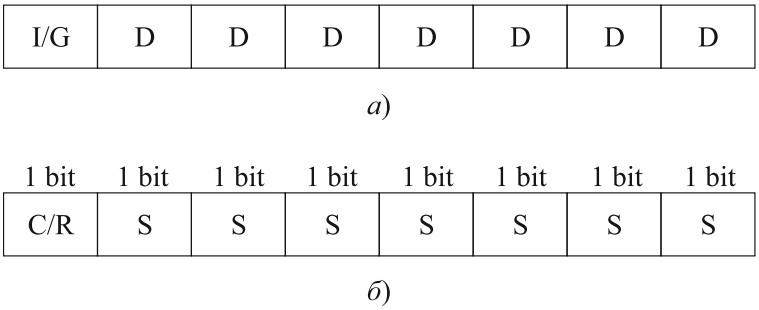


Рис. 2.12 – Структура адресов *а*) DSAP и *б*) SSAP: D — бит адреса службы места назначения; S — бит адреса службы отправителя

Протокол доступа к подсети (Sub-Network Access Protocol, SNAP) был разработан с целью увеличения числа поддерживаемых протоколов, так как однобайтные поля SAP позволяют поддерживать не более 256 протоколов.

В принципе, он часто применяется для передачи кадров Ethernet по сетям с другой топологией. Формат Ethernet SNAP предусматривает дополнительное пятибайтное поле для идентификации протокола (Protocol Identification, PI) внутри поля данных, причем первые три байта представляют собой код производителя, как правило, совпадающий с первыми тремя байтами адреса отправителя (vendor code), хотя иногда они равны нулю. Значения двух последних байтов этого поля совпадают со значениями поля протокола в Ethernet II в случае, если кадры содержат пакеты одного и того же высокоуровневого протокола, например они равны 0×8137 для NetWare.

Определение типа кадра

Сети передачи данных зачастую гетерогенны, т. е. одновременно используется несколько протоколов, например TCP/IP и Novell IPX. В этом случае важной задачей является корректное определение типа кадра (табл. 2.1).

Таблица 2.1 – Протоколы и соответствующие типы кадров

Формат кадра	**Протокол**	**Способ идентификации**
Ethernet II	DECnet, старые реализации TCP/IP	Поле типа протокола
IEEE 802.3	Novell Net Ware 3.x	Первые два байта поля данных равны 0FFFFh
IEEE 802.2	Novell Net Ware 4.x	Поле DSAP
IEEE 802.2 SNAP	EtherTalk, новые реализации TCP/IP	Пятибайтное поле после служебной информации

2.5 Схемы и оборудование сетей Ethernet

2.5.1 Стандарт 10Base-T

В этом разделе описаны технологии сетей с равноправным доступом (сети на хабах). В настоящее время эти технологии практически не применяются и приведены здесь с целью изложения процессов развития сетевых технологий.

Схема сети приведена на рисунке 2.13. Здесь компьютеры подключаются к хабу через сетевую карту — NIC (Network Interface Controller) и две пары многопарного неэкранированного кабеля типа UTP (Un-shielded Twisted Pair). На схеме *TX* — выход передатчика, *RX* — вход приемника.

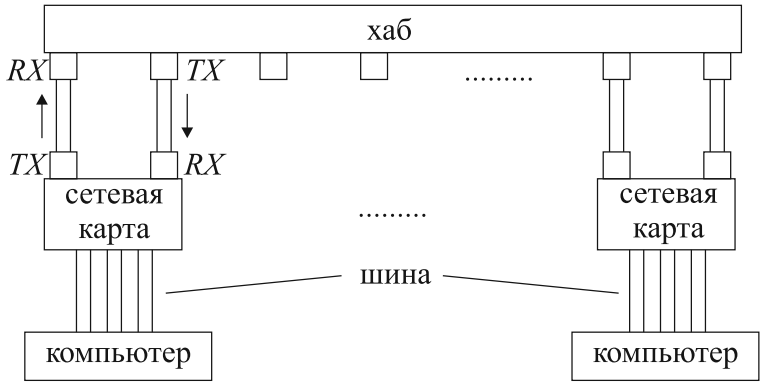
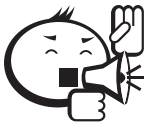


Рис. 2.13 – Схема ЛВС



Достоинства схемы 10Base-T:

- удобство монтажа, поскольку он осуществляется по схеме «звезда» с применением стандартных 8-контактных разъемов RJ-45;
- повреждения кабеля не выводят из строя всю сеть;
- повреждения легко обнаруживаются;
- возможен плавный переход на технологию Fast Ethernet;
- концентратор (хаб) является интеллектуальным устройством, что позволяет ему обеспечивать в сети ряд дополнительных функций, таких как ретрансляция кадров и обнаружение коллизий.

Рассмотрим функции и характеристики элементов подробней.

Сетевая карта:

- сопрягает сеть с компьютером, преобразовывая параллельный код в последовательный через шины ISA (8, 16 разрядов, скорость 64 Мбит/с), PCI (32, 64 разряда, скорость 2112 Мбит/с);

- кодирование и декодирование сигналов (Манчестер II и др.);
- идентификация своего адреса в принимаемом пакете;
- выявление коллизий;
- выявление ошибок (подсчет контрольной суммы);
- промежуточное хранение данных и служебной информации в буфере. Это позволяет возложить функции контроля над сетью на сетевую карту;
- согласование скорости передачи данных от компьютера в сеть;
- гальваническая развязка кабеля и устройства карты с помощью импульсного трансформатора или оптрона.

Кабель на витой паре

Среди разнообразия кабелей с витыми парами наибольшее распространение получили кабели UTP категорий 3, 4, 5. В этих кабелях содержится 4 неэкранированные скрученные пары проводов. Каждая пара имеет волновое сопротивление 100 Ом. Основное различие между категориями заключается в полосе пропускания частотной характеристики и допустимой длине сегмента (табл. 2.2).

Таблица 2.2 – Характеристики кабелей UTP

Тип кабеля	**Характеристики**	
	Полоса пропускания, МГц	**Длина сегмента, м**
UTP-3	15	100
UTP-4	20	120
UTP-5	100	150
UTP-6 (экранированная)	300	150

Наибольшей полосой пропускания и помехоустойчивостью обладает экранированная витая пара (категории 6, 9). Из четырех пар для подключения к хабам и сетевым картам используются только две. Остальные пары свободны и могут быть применены для телефонии. В стандарте 10Base-T оговаривается максимальная длина сегмента — 100 м. Для максимальной длины допустимое затухание в кабеле составляет 14 дБ на частоте 15 МГц и ослабление перекрестной помехи между соседними парами не менее 30 дБ на частоте 5 МГц и 23 дБ на частоте 15 МГц.

Концентратор обеспечивает следующие функции:

- ретрансляция принимаемых сигналов на все другие порты с восстановлением амплитуды и формы сигнала (рис. 2.14);
- обнаружение коллизий и передача сигнала «пробка» на все порты;
- исправление ошибки «ложная несущая», когда пакет приходит без преамбулы, он выявляется и данный порт отключается;
- исправление ситуации «множественная коллизия» — более 60 коллизий подряд. Такой порт отключается, а потом включается снова;
- исправление ситуации «затянувшаяся передача», когда сеанс длится более 4 миллисекунд.

Концентраторы Ethernet могут иметь от 8 до 72 портов.

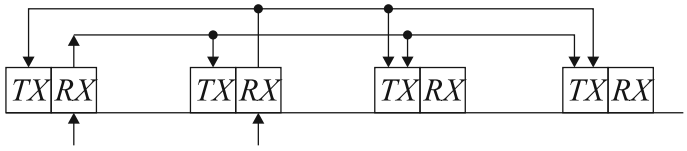


Рис. 2.14 – Ретрансляция сигналов в хабе

В ЛВС с большим числом станций, которых не должно быть больше чем 1024, концентраторы могут включаться каскадно (см. рис. 2.15).

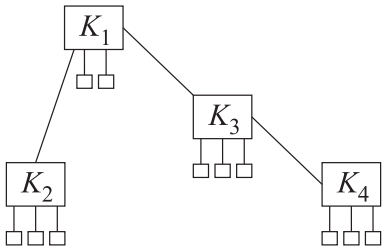


Рис. 2.15 – Каскадное включение хабов

При этом диаметр сети (максимальное расстояние между двумя компьютерами) не должен превышать 500 м. Это требование связано с условием затухания сигнала, и из него следует важное правило 4-х хабов: между двумя любыми компьютерами не должно находиться более четырех хабов. Это правило основывается на том, что длина сегмента не должна превышать 100 м, а диаметр сети 500 м.

2.5.2 Стандарт 10Base-FL

Использование ВОЛС дает следующие преимущества:

- вследствие малого затухания существенное увеличение длины сегмента. Так, при многомодовом волокне она составляет 2000 м. Для одномодового волокна она ограничивается только длиной домена коллизий, равной 2500 м. Затухание ограничивает длину до 100 км;
- повышение помехоустойчивости, так как электрические помехи и наводки отсутствуют, а искажения формы оптических импульсов на тактовых частотах в 10 МГц незначительны;
- автоматическая гальваническая развязка между сетевой картой и концентратором за счет преобразования электрического сигнала в оптический и обратно;
- возможность перехода на более скоростные технологии Fast Ethernet и Gigabit Ethernet.

Схема сети Fast Ethernet приведена на рисунке 2.16.

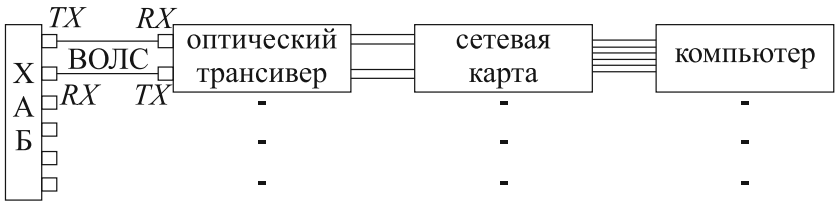


Рис. 2.16 – Схема сети на ВОЛС

Здесь между сетевой картой и хабом включен оптический трансивер или конвертор, который электрические импульсы, поступающие от сетевой карты, преобразует в оптические, и наоборот. Между оптическими портами хаба и трансивера включена ВОЛС.

Требования к многомодовым оптическим кабелям, которые преимущественно применяются в Fast Ethernet: длина волны λ = 0.85 мкм — ближний ИК диапазон, потери в кабеле 4–5 дБ/км, потери в оптическом разъеме 0.5–2 дБ. Таким образом, суммарные потери в оптическом сегменте не должны превышать 12.5 дБ.

2.5.3 Общие характеристики стандарта Ethernet

Номинальная пропускная способность — 10 Мбит/с.

Максимальное число станций — 1024, остальные характеристики приведены в таблице 2.3.

Таблица 2.3 – Характеристика сетей Ethernet

Характеристики	**Стандарт**	
	10Base-T	**10Base-F**
Кабель	Неэкранированная витая пара UTP	Многомодовое волокно — MM
Максимальное расстояние между узлами сети	500 м	2500 м
Максимальная длина сегмента	100 м	2000 м
Максимальное число хабов	4	4

2.6 Производительность сети Ethernet

При оценке производительности сети будем различать максимальную производительность (пропускную способность) и реальную производительность обмена между двумя станциями.

1. Максимальная производительность реализуется при работе в сети только двух абонентов с максимально возможной скоростью.

Производительность снижается за счет:

- служебной информации (заголовков),
- IPG.

Наибольшее влияние этих факторов проявляется для кадров минимальной длины (72 байта), так как удельный вес полезной информации (46 байт) наименьший. В этом случае число коротких кадров, передаваемых в секунду

$$n_k = \frac{1}{(72 \cdot 8 + 96) \cdot 10^{-7}} = 14\ 880 \text{ кадров/с.}$$

Пропускная способность находится только из учета информационных байтов в пакете

$$C_{nk} = 14\ 880 \cdot 46 \cdot 8 = 5.48 \text{ Мбит/с.}$$

Эффективность передачи

$$\eta_k = \frac{c_{nk}}{c_{n\max}} = 0.548.$$

Для кадров максимальной длины (1500 байт)

$$n_g = \frac{1}{(1526 \cdot 8 + 96) \cdot 10^{-7}} = 812 \text{ кадров/с.}$$

$$C_{ng} = 9.76 \text{ Мбит/с, а } \eta = 0.976.$$

Таким образом, максимальная производительность для самых длинных кадров приближается к 100%.

2. Реальная производительность. При одновременно работающих станциях производительность вначале (при малом N) делится между ними пропорционально. С ростом нагрузки (объем передаваемой информации) вначале производительность растет линейно, а затем начинают возникать коллизии, и рост реальной производительности замедляется (рис. 2.17). При нагрузке сети 0.7–0.8 возникает коллапс сети. Она не передает информацию, а занимается только устранением коллизий.

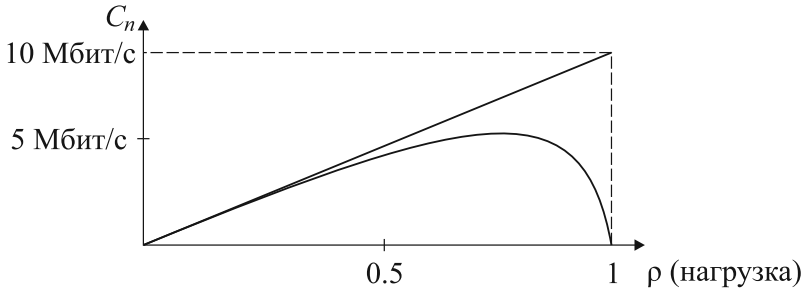


Рис. 2.17 – Реальная производительность сети Ethernet

На практике достижение реальной производительности в 3–4 Мбит/с считается хорошим показателем.

2.7 Fast Ethernet

Быстрое развитие технологии Ethernet, рост числа пользователей, развитие прикладных процессов, требующих передачи больших объемов информации (передача

файлов, видео и т. п.), с одной стороны, и простота технологий, ее экономическая привлекательность — с другой, предопределили появление следующего более скоростного стандарта — Fast Ethernet со скоростью 100 Мбит/с (IEEE 802.3u).

Само присутствие в названии новой технологии слова Ethernet означает высокую преемственность.

Что осталось неизменным в Fast Ethernet?

1. Способ доступа — *CSMA/CD*.
2. Форматы кадров.
3. Подуровни *MAC* и *LLC*.
4. Поскольку скорость передачи возросла в 10 раз, то в 10 раз уменьшилось значение биттайма *BT* = 10 нсек и все остальные величины, связанные по времени. Наиболее серьезные ограничения касаются диаметра сети. Поскольку время двойного оборота сократилось до ~ 5.2 мкс, диаметр домена тоже уменьшился до 200 м.
5. Fast Ethernet также использует топологию «звезда» либо в полудуплексном режиме (с концентратором), либо в дуплексном режиме (с коммутатором).

Все изменения произошли на физическом уровне. Они вызваны тем, что при увеличении скорости передачи информации в 10 раз и сохранении длины сегмента 100 м надо компенсировать увеличившееся за счет расширения полосы частот затухание сигнала.

На физическом уровне различают четыре версии.

100Base-TX — наиболее популярная версия. Реализуется на витой паре UTP-5, которая обеспечивает полосу пропускания 100 МГц, и поэтому для Fast Ethernet достаточно двух пар проводов. Разъемы соответствуют стандарту 10Base-T, что дает нужную совместимость Ethernet ~ Fast Ethernet. В качестве линейного кода использовался MLT-3, заимствованный из технологии FDDI. Код MLT-3 — трехуровневый, усложненный вариант NRZ ЧПИ. При передаче «0» значение не меняется, при передаче «1» значения меняются по цепочке +V, 0, −V, 0, +V (рис. 2.18).

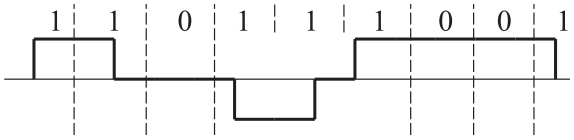


Рис. 2.18 – Код MLT-3

Этот код благодаря биполярному характеру сигнала и свойствам NRZ имеет меньшую ширину спектра.

Для логического кодирования применен код 4B/5B, который исключает наличие большого количества «0», следующих подряд. Суть этого кода поясняется в таблице 2.4.

Поскольку число комбинаций выходного кода гораздо больше, то «лишние» комбинации считают запрещенными, и их появление сигнализирует об ошибках. Сочетание кодов MLT-3 и 4B/5B, по сравнению с манчестерским кодом, обеспечивает при равной пропускной способности меньшую полосу пропускания в 8/5 раза. Это объясняется тем, что для манчестерского кода длительность минимального

импульса равна половине тактового интервала, в то время как для MLT-3 они равны (выигрыш в 2 раза). Применение кода 4B/5B уменьшает требуемую скорость в 5/4 раза $(2 : 5/4 = 8/5)$.

Таблица 2.4 – Пример кодирования 4B/5B

Входной сигнал	Выходной сигнал
0 0 0 0	1 1 1 1 0
0 0 0 1	0 1 0 0 1
0 0 1 0	1 0 1 0 0
. . .	. . .
1 1 1 1 1	1 1 1 0 1

100Base-T4 — эта версия может быть реализована даже на витой паре категории 3 (UTP-3), несмотря на то, что частотный диапазон такого кабеля составляет всего 16 МГц. Для того, чтобы обеспечить скорость передачи 100 Мбит/с при такой полосе частот, применяют следующие меры.

Однонаправленная параллельная передача сразу по трем парам. При этом необходимая скорость уменьшается до 33.3 Мбит/с.

Применение биполярного кода 8B/6T, когда комбинация двоичного кода из 8 бит передается шестью символами, имеющими три значения: «+», «–», и 0. Поскольку в выходном сигнале кодера длительность импульса возрастает в 8/6 раза, то требуемая пропускная способность при физической скорости 33.3 Мбит/с достигает 25 Мбит. Другой важной особенностью сигнала 8B/6T является то, что его частотный спектр укладывается в полосу пропускания 16 МГц, что достаточно для кабеля UTP-3. Четвертая пара в кабеле UTP-3 используется для прослушивания сети. При появлении в ней сигнала при собственной передаче делается заключение о наличии коллизии.

Основным недостатком технологии 100Base-T4 является полудуплексный режим работы, а ее применимость объясняется тем, что она обеспечивает самый простой переход со стандарта 10Base-T.

100Base-FX — это версия для многомодового волокна с длиной волны λ = = 1.3 мкм. Здесь применяется логическое кодирование 4B/5B, как и в 100Base-TX, и физический код *NRZI*. Передача и прием могут вестись как в полудуплексном, так и в полнодуплексном режимах по двум волокнам. В случае полудуплексного режима размер сети ограничивается коллизиями — 412 м, а в режиме *full duplex* — затуханием (2 км для многомодового волокна и 32 км для одномодового). Переход со 100Base-FX на 10Base-FL невозможен, поскольку стандарт 10Base-FL рассчитан на λ = 0.83 мкм.

100Base-SX — версия на недорогих светодиодах (λ = 0.83 мкм) и многомодовом волокне. Это позволяет реализовать совместимость с 10Base-FL, но при этом уменьшается дальность до 300 м. Это дешевая альтернатива 100Base-FX.

Основные характеристики интерфейсов Fast Ethernet приведены в таблице 2.5.

Проектирование сетей Fast Ethernet в пределах домена коллизий (на хабах) не требует расчетов и предлагает проектировщикам четыре стандартных варианта.

Вариант 1А (без хаба). Здесь рассматривается соединение «точка-точка» двух узлов. В качестве узлов могут выступать рабочая станция, сервер, коммутатор.

В этом случае необходимо обеспечить требования только по максимальному расстоянию (табл. 2.5, строка 6).

Таблица 2.5 – Характеристики стандарта Fast Ethernet

Характеристики	100Base-FX	100Base-TX	100Base-T4
1. Порт устройства	*Duplex SC*	*RJ-45*	*RJ-45*
2. Среда передачи	ВОЛС (мм)	*UTP*-5	*UTP*-3, 4, 5
3. Число пар (волокон)	2	2	4
4. Линейный код	*NRZI*	*MLT*-3	ЧПИ
5. Логический код	4B/5B	4B/5B	8B/6T
6. Максимальная длина сегмента	$\leqslant$ 412 м (мм) $\geqslant$ 2 км (мм, FD)	100 м	100 м

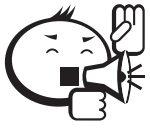
Вариант 1B. Этот вариант предполагает применение хаба класса 1 с задержкой на двойном пробеге не более 130 BT. В этих хабах допускаются порты T4, TX, FX. Поскольку из-за трансляции протоколов задержка достаточно большая, то может использоваться только один хаб, а расстояние от станций до хаба не более 100 м. При этом диаметр сети 200 м.

Вариант 1C. Здесь применяются хабы класса 2, у которых задержка по портам TX/FX — 46 BT, а для портов T4 — 33.5 BT. Поэтому допускается соединение двух хабов с расстоянием между ними 5 м. Максимальная длина сегментов на витой паре 100 м, на оптоволокне — 136 м.

Небольшое количество хабов не препятствует развитию сетей Fast Ethernet поскольку наряду с хабами используются коммутаторы, которые делят сеть на отдельные домены коллизий. Общая длина сети может быть в этом случае достаточно большой.

2.8 Коммутируемый Ethernet

Развитие технологии ЛВС и сетей Ethernet происходило на базе применения коммутаторов.



Коммутатор — это многопортовое устройство, содержащее (рис. 2.19) коммутационную матрицу, входные и выходные порты и процессорный блок.

Каждый порт имеет буферную память и свой процессор. При поступлении пакета процессор порта отправляет в буфер байты, содержащие адрес получателя. Информация об адресах отправителя и получателя поступает в процессорный блок. Там по адресной таблице определяется номер выходного порта и формируется команда для коммутационной матрицы о создании соответствующего пути между входными и выходными портами (табл. 2.6). Если таблица не содержит адреса получателя, то он записывается в новой строке, пакет широковещательно передается через все порты, кроме входного, принявшего пакет.

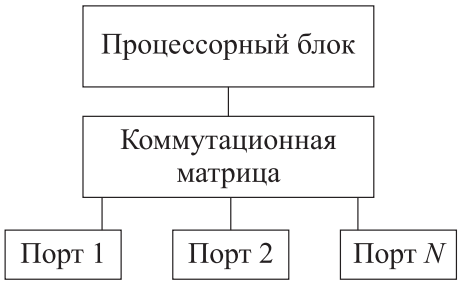


Рис. 2.19 – Схема коммутатора

Таблица 2.6 – Адресная таблица

MAC-адрес	№ порта
A	1
B	2
C	3
D	4

В адресной таблице каждому MAC-адресу сопоставляется порт коммутатора. К каждому порту может быть приписан один или несколько адресов. Так, например, (рис. 2.20) станция *A* посылает пакет к порту 1. Процессор коммутатора анализирует адрес получателя (*D*) и идентифицирует его с соответствующим портом коммутатора 4. По команде процессора коммутатор создает путь между портами 1 и 4 и посылает пакет на выходной порт. Вместо отдельных станций *A*, *B*, *C*, *D* могут быть включены целые сегменты на хабах.

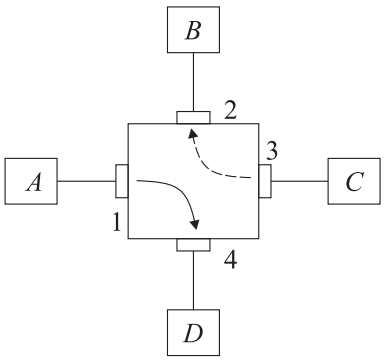


Рис. 2.20 – Сеть с коммутатором

Рассмотренный алгоритм работы коммутатора помогает понять основные его преимущества при создании компьютерных сетей.

1. Сегментация сетей. Если в сети, состоящей из нескольких хабов, вместо одного из них включить коммутатор (рис. 2.21), то коммутатор будет транслировать пакеты из подсети 1 к станциям подсетей $2, 3, \ldots, N$. Пакеты, которые предназначены станциям подсети 1, пропускаться не будут. Соответственно будет осуществ-

ляться фильтрация пакетов всех остальных подсетей. Число пакетов, поступающих на каждую станцию, резко уменьшится, что значительно уменьшит вероятность коллизий. Таким образом, коммутатор разбивает большой домен коллизий на несколько сегментов.

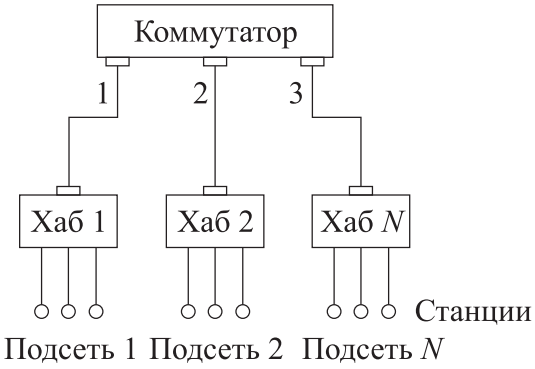


Рис. 2.21 – Сегментация ЛВС

2. Одновременное соединение нескольких сетей. Если обратиться к рисунку 2.23, то можно заметить, что наряду с соединениями 1–4, коммутационная матрица позволяет одновременно реализовать соединение 3–2. В общем случае для N портов может быть получено $N/2$ соединений. Это приводит к увеличению в $N/2$ раз пропускной способности. С другой стороны, при широковещательной рассылке (например, от 1 к 2, 3, 4) увеличения пропускной способности не происходит.

3. Построение виртуальных локальных сетей (VLAN). Виртуальной сетью называется группа станций, находящихся в общей сети, трафик которой на канальном уровне передается только между станциями этой группы. Создание VLAN с помощью коммутаторов не требует каких-либо физических переключений. Поэтому они называются виртуальными. Отдельные VLAN могут связываться между собой через устройства третьего уровня — маршрутизаторы. Основные принципы построения виртуальных сетей регламентируются стандартом *IEEE 802.1Q*.

Существует три подхода при построении VLAN. Первый основан на объединении станций через порты коммутатора. Обратившись к рисунку 3.23 и задав там через процессор постоянное соединение 1–4 и 2–3, можно отметить, что все станции сегментов *B* и *C* образуют одну VLAN, а станции сегментов *A* и *D* другую. Недостатком такого способа является то, что в пределах одного сегмента нельзя выделить какую-то одну станцию или группу для включения в VLAN. Достоинством является простота создания виртуальной сети, не требующая большого объема ручной работы администратора.

Второй подход основан на объединении станций с помощью их MAC-адресов. При этом любая станция VLAN может подключаться к любому порту коммутатора. Принадлежность станций к конкретной VLAN заносится в процессор коммутатора, который и разрешает коммутатору пересылку пакетов в пределах каждой виртуальной сети. Этот метод требует от администратора большого объема ручной работы.

Предыдущие два подхода основаны только на добавлении дополнительной информации к адресным таблицам моста и не используют возможности встраивания информации о принадлежности кадра к виртуальной сети в передаваемый кадр.

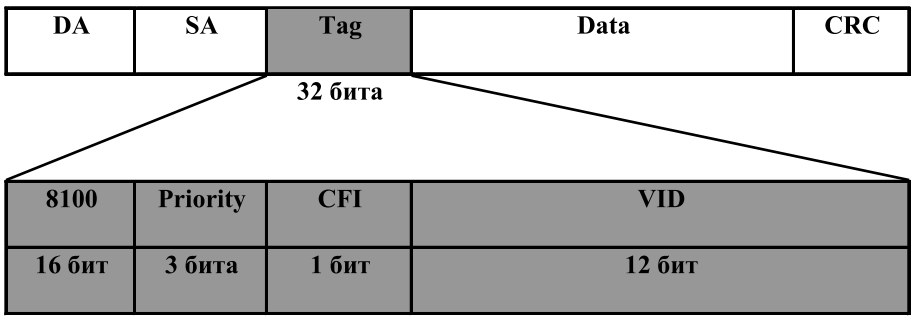
Метод организации VLAN на основе меток — тэгов — использует дополнительные поля кадра для хранения информации о принадлежности кадра при его перемещениях между коммутаторами сети.

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети (табл. 2.7). К кадру Ethernet добавлены четыре байта. Первые два байта с фиксированным значением 0×8100 определяют, что кадр содержит тег протокола 802.1Q/802.1p. Остальные два байта содержат следующую информацию:

- 3 бита приоритета передачи кодируют до восьми уровней приоритета (от 0 до 7, где 7 — наивысший приоритет), которые используются в стандарте 802.1p;
- 1 бит Canonical Format Indicator (CFI), который зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- 12-битный идентификатор VLAN, определяющий, какой VLAN принадлежит трафик.

Таблица 2.7 – Структура и положение тега в кадре Ethernet: DA — адрес назначения, SA — адрес источника

Кадр Ethernet IEEE 802.1Q



С точки зрения удобства и гибкости настроек VLAN на основе меток является лучшим решением.

Основные преимущества третьего подхода состоят в следующем:

1. Гибкость и удобство в настройке и изменении — можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта 802.1Q. Способность добавления меток позволяет VLAN распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению.
2. Позволяют активизировать алгоритм покрывающего дерева (Spanning Tree) на всех портах и работать в обычном режиме. Протокол Spanning Tree оказывается весьма полезным для применения в крупных сетях, построенных на нескольких коммутаторах, и позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей

или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола Spanning Tree коммутаторы после построения схемы сети блокируют избыточные маршруты, таким образом автоматически предотвращается возникновение петель в сети.

3. Способность VLAN 802.1Q добавлять и извлекать метки из заголовков пакетов позволяет VLAN работать с коммутаторами и сетевыми адаптерами серверов и рабочих станций, которые не распознают метки.
4. Устройства разных производителей, поддерживающие стандарт, могут работать вместе, т. е. независимо от какого-либо фирменного решения.
5. Не нужно применять маршрутизаторы, чтобы связать подсети на сетевом уровне, достаточно включить нужные порты в несколько VLAN для возможности обмена трафиком. Например, для обеспечения доступа к серверу из различных VLAN, нужно включить порт коммутатора, к которому подключен сервер, во все подсети. Единственное ограничение — сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.
6. Поддержка полнодуплексного режима (*full duplex*).

Почти все сегменты ЛВС (за исключением 100Base-T4) имеют возможность передавать сигналы по двум линиям (рис. 2.22), так как и сетевые карты, и концентраторы имеют по два порта (*TX* и *RX*). Однако алгоритм CSMA/CD ограничивает функционирование сети только полудуплексным режимом. Ситуация коренным образом меняется при переходе к коммутаторам, которые тоже имеют порты передатчика и приемника.

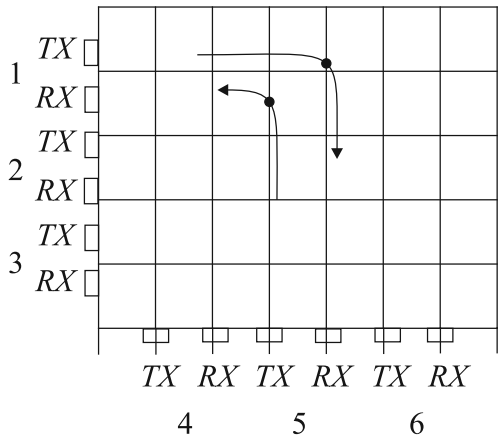


Рис. 2.22 – Полный дуплекс в коммутаторе

При создании коммутационного пути (рис. 2.22) входные и выходные порты соединяются попарно $TX_1 \rightarrow RX_5$ и $TX_5 \rightarrow RX_1$, обеспечивая двухстороннюю передачу.

Понятие «общая шина» или «логическая шина» здесь перестает действовать, поскольку пакеты разделены портами. Если каждая станция подключена к своему порту коммутатора (концентраторы отсутствуют), проблема коллизий исключается и режим *full duplex* реализуется полностью для каждой пары портов.

Существуют разные режимы работы коммутаторов.

1. Коммутация «напролет» — Cut through. В этом случае считывается только адрес назначения и сразу начинается передача на выходной порт. Анализ всего пакета не производится. В силу этого такие коммутаторы самые простые и быстродействующие. Время задержки пакета складывается из задержки на запись (6 байт адреса) и задержки непосредственно на коммутацию и составляет не более 150 BT. Помимо этого каждый порт коммутатора может обнаруживать коллизии в своем сегменте и ликвидировать их.

К недостаткам режима «напролет» относятся:

- передача ошибочных пакетов (с неправильной контрольной суммой и т. п.) и «карликовых» пакетов (< 512 BT);
- невозможность передавать пакеты, поступающие сразу с разных входных портов на один выходной порт. Часть пакетов при этом пропадает.

2. Бесфрагментная коммутация. Это усовершенствованный вариант режима «напролет» и отличается тем, что все порты имеют объем памяти FIFO 512 бит, что позволяет записывать самые короткие пакеты. Если пакет заканчивается раньше, чем заполнится буфер, то содержимое буфера отбрасывается. Так решается проблема «карликовых» пакетов. Все остальные недостатки режима «напролет» остаются. Время задержки пакета в таком коммутаторе увеличивается до 400 BT.

3. Коммутация с полной буферизацией (Store-and-Forward) — SAF. В этом режиме записываются все, даже самые длинные пакеты (1500 байт). Соответственно, задержка существенно возрастает и может составить 12 000 BT. Ошибочные и карликовые пакеты здесь отбрасываются, а перегрузки возникают гораздо реже, поскольку в таких коммутаторах процессоры имеются не только в передатчиках и приемниках портов, но и в самом коммутаторе (общая часть). Такой процессор регулирует поступление пакетов на порты и не допускает перегрузок, управляя памятью и скоростью передачи.

Коммутаторы с полной буферизацией могут одновременно поддерживать разные скорости передачи 10 Мбит/с и 100 Мбит/с. Поэтому часть портов может работать в режиме Ethernet, а часть — в режиме Fast Ethernet.

Кроме вышеперечисленного, также можно отметить гибридные коммутаторы, которые автоматически переключаются из режима «напролет» в режим полной буферизации и наоборот. При малой нагрузке и при низком уровне ошибок они переходят в более скоростной режим «напролет». К основным характеристикам коммутаторов относятся его производительность, количество портов, размер адресной таблицы, объем буферной памяти.

Наиболее емкой характеристикой является производительность. Она включает в себя такие составляющие:

- скорость фильтрации (уничтожения) кадров;
- скорость передачи кадров;
- пропускная способность;
- задержка передачи кадра.

Среди этих характеристик наиболее универсальной и показательной является пропускная способность, поскольку она не зависит от размера кадра и измеряется в битах в секунду. В соответствии со стандартом Ethernet эта величина составляет

10 Мбит/с или 100 Мбит/с при передаче кадров через один порт. Разумеется, что приближение к этим цифрам ближе всего реализуется на кадрах максимальной длины. Кроме этой характеристики, применяют другую — суммарную производительность или суммарную пропускную способность по всем его портам.

Задержка передачи кадра рассматривалась ранее. Для Ethernet она составляет от 5 до 40 мкс для коммутации «напролет» и от 50 до 400 мкс для кадров минимальной длины при полной буферизации.

Количество портов коммутатора не бывает большим и меняется от 6 до 24. Это не влияет на количество станций, задействованных в одной ЛВС, так как коммутаторы могут включаться по древовидной схеме и на одном порту может прописано большое количество MAC-адресов.

Размер адресной таблицы определяется из расчета на один порт. Здесь различают несколько вариантов. Если коммутатор предназначен для организации рабочей группы, то число MAC-адресов на один порт составляет несколько единиц. В распространенном случае режима *full duplex*, когда коммутатор обслуживает магистраль, число MAC-адресов на порт составляет 4000–8000.

Буферные устройства коммутаторов предназначены для временного хранения кадров, в тех случаях, когда их нельзя передать сразу на выходной порт. Такие ситуации возникают при пиковых нагрузках, когда кадры поступают одновременно на все входы и не могут быть переданы на выходные порты. Для того чтобы потери трафика были минимальными, объем памяти на каждом порту должен быть достаточно большим. Обычно для ответственных сегментов сети применяют коммутаторы с объемом памяти в десятки и сотни килобайт на порт. Дополнительным средством буферизации является память центрального процессора объемом в несколько мегабайт.

В коммутаторах предусмотрен контроль и регулирование скорости входных потоков с целью избегания перегрузок. Широко известен способ «обратного давления» (рис. 2.23). Пусть порты 1, 2, 3 коммутатора передают пакеты на порт 4. При определенной суммарной скорости $V_{\text{пер}}$ порт 4 не справляется с передачей всех трех входных потоков и входные буферы портов 1–3 начинают переполнятся. Это приводит к отбрасыванию «лишних» кадров и существенному снижению скорости передачи. Чтобы искусственно снизить скорость передачи на входах, коммутатор посылает в сегменты 1, 2, 3 «пустые» кадры (кадры, не несущие информации), которые воспринимаются как наличие коллизий. Это замедляет скорость передачи.

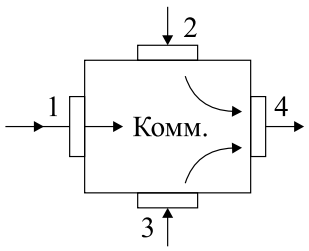


Рис. 2.23 – Регулирование перегрузки

Рассмотрим основные схемы построения сетей на основе коммутаторов (рис. 2.24). Их можно разделить на две группы: с применением комбинации коммутаторов и концентраторов (*а*) и на одних коммутаторах (*б*). Несмотря на их топологиче-

скую схожесть, эти схемы имеют принципиальные различия. Первая имеет в своем составе домены коллизий и может работать только в полудуплексном режиме. Порты коммутатора включены соответственно в свои сегменты и тоже должны поддерживать полудуплексный режим. Возникновение коллизий снижает производительность сети при достаточно большом количестве станций в сегментах. Единственным достоинством такой схемы является ее низкая стоимость. Поэтому применяется она для построения сетей небольших рабочих групп, не требующих высоких скоростей обмена и не предполагающих существенных изменений объемов трафика.

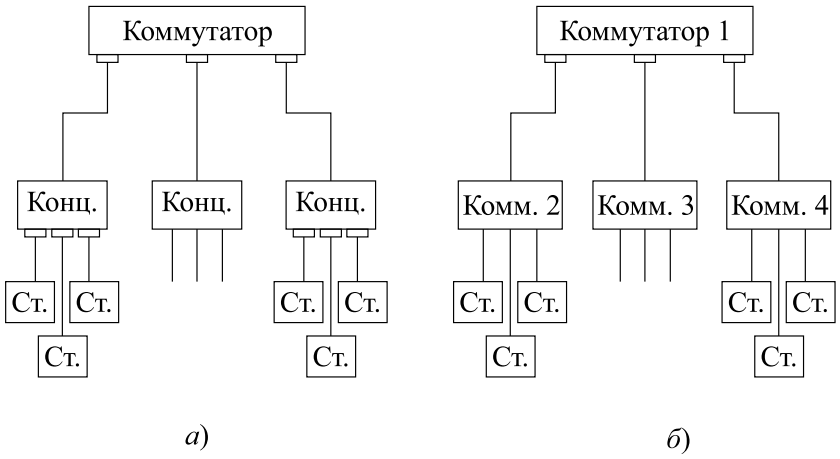


Рис. 2.24 – Схемы сетей с применением коммутаторов: *а*) коммутатор — концентратор; *б*) коммутатор — коммутатор

Вторая схема более прогрессивна, так как работает в режиме *full duplex*. Обозначим еще раз достоинства этого режима. Поскольку коллизии отсутствуют, то сеть нормально работает при нагрузке, приближающейся к 100% от пропускной способности. Ограничения на размер сети здесь уже будут определяться только физическими характеристиками среды передачи (затухание и дисперсия). Ограничения, связанные со временем двойного оборота, автоматически снимаются. Поэтому при использовании оптоволоконной линии длина сегмента для Fast Ethernet может составлять 2 км и более.

В схеме на коммутаторах необходимо сочетание медленных (Ethernet) и быстрых (Fast Ethernet) портов. Это надо для того, чтобы станции одновременно могли обращаться к одному и тому же сетевому устройству (например, серверу) без снижения скорости. Поэтому порт, к которому подключается сервер, должен быть высокоскоростным.

В силу своих преимуществ схемы на коммутаторах вытесняют схемы с применением концентраторов.

К *недостаткам* схем на коммутаторах относятся:

- ограниченное количество абонентов в одном узле (небольшое число портов);
- увеличение затрат на построение сети;
- невозможность организовать кольцевые и ячеистые сети.

Рассмотрим последнее ограничение подробно. Пусть схема на коммутаторах (рис. 2.25) работает в режиме *full duplex*. Петля образуется при соединении комму-

таторов K_2 и K_3. Предположим, что к коммутатору K_2 подключилась новая станция с MAC-адресом 7. Тогда в таблице K_2 появится запись

K_2	MAC-адрес	Порт
	7	2

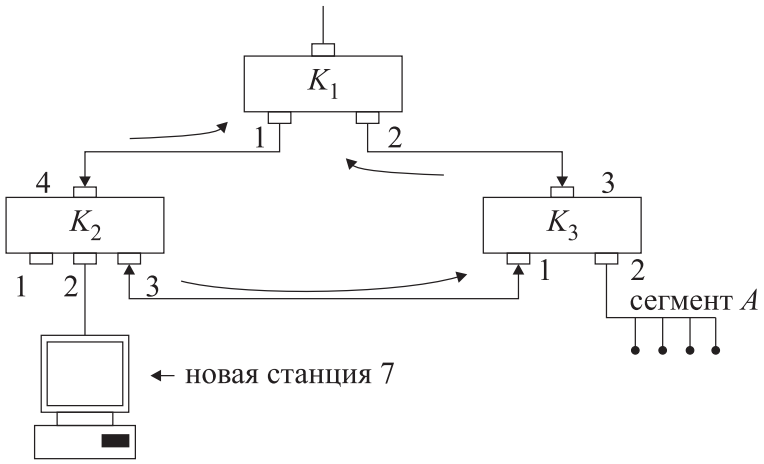


Рис. 2.25 – Образование замкнутых маршрутов

Коммутатор K_2 начинает широковещательную рассылку новой информации. Поэтому в таблицах K_1 и K_3 появятся записи.

K_1	MAC-адрес	Порт
	7	1

K_3	MAC-адрес	Порт
	7	1

K_1 и K_3 также ведут широковещательную рассылку этой информации. При этом информация о станции 7 придет на порт 2 K_1 от K_3. Поскольку эта информация более свежая, то старая запись будет заменена новой.

K_1	MAC-адрес	Порт
	7	2

Аналогично для K_3 замена будет следующей

K_3	MAC-адрес	Порт
	7	3

Наличие петли приводит к следующим отрицательным результатам:

- размножение кадра (появляются две копии);
- появление излишнего трафика (обе копии циркулируют по петле в противоположных направлениях);
- постоянная смена таблиц в коммутаторах.

Все это вынуждает использовать в сетях с коммутаторами древовидные структуры. Такие структуры достаточно легко реализуются в простых сетях с небольшим количеством коммутаторов и ненапряженным трафиком. В сложных сетях возможно появление петель либо непреднамеренно, либо специально для организации резервных путей или регулировки трафика. Для исключения петель в таких схемах некоторые активные порты блокируют вручную или автоматически.

Наиболее распространенным способом автоматического выключения избыточных связей является алгоритм «покрывающего дерева» — *Spannig Tree Algoritm* (*STA*). Суть этого алгоритма заключается в следующем. Коммутатор постоянно тестирует сеть и, опрашивая соседние коммутаторы, создает активную древовидную структуру. При этом коммутатор автоматически обнаруживает отказы портов, кабеля и т. п.

Процедура *STA* следующая:

1. Определение корневого коммутатора, от которого строится дерево (обычно он назначается администратором сети).
2. Для каждого коммутатора определяется корневой порт. Это такой порт, который обеспечивает соединение с корневым коммутатором по кратчайшему пути.
3. Для каждого сегмента сети выбирается назначенный порт, имеющий кратчайшее расстояние до корневого коммутатора.

Так, например, для сети, изображенной на рисунке 2.25, корневым коммутатором может быть выбран K_1. Для коммутатора K_3 корневым портом является порт 3, а назначенным портом для сегмента A — порт 2. Для устранения петли порт 1 K_3 или порт 3 K_2 должны быть заблокированы.

Помимо реализации алгоритма *STA* коммутаторы могут обеспечить и другие дополнительные функции — фильтрации и приоритезации трафика. Обычно фильтрация осуществляется по отношению к станциям сети и заключается в создании запретов на прохождение пакетов либо к определенным портам, либо к определенным типам сервисов. Наиболее просто реализуются фильтры на основе MAC-адресов. Для этого в адресной таблице организуются дополнительные позиции, в которых прописываются условия фильтрации, например отбрасывание кадров с определенным адресом. Другими примерами фильтрации являются запреты на доступ к отдельным видам разделяемых ресурсов: печать, доступ в Интернет и др.

Приоритетная обработка кадров заключается в том, что коммутатор, используя буфер, может по каждому входному и выходному портам вести не одну, а несколько очередей с различными приоритетами. Это позволяет обеспечить разное качество обслуживания по задержке и пропускной способности.

Поскольку у кадров Ethernet нет поля приоритетов, коммутатор должен использовать дополнительные механизмы. Один из этих механизмов — присвоение приоритетов портам коммутатора. На выходном порту пакеты выстраиваются в разные очереди в зависимости от номера входного порта. В этом случае все станции, подключенные к одному порту, будут иметь одинаковый приоритет.

Более гибкое присвоение приоритетов заложено в протоколе IEEE 802.1p. Он предусматривает дополнительный заголовок на 16 бит, в котором 3 бита используются для указания приоритета.

2.9 Gigabit Ethernet

Переход локальных вычислительных сетей на скоростную технологию Fast Ethernet привел к перегрузке в сегментах с общим ресурсом (рис. 2.26). Здесь приведена упрощенная структура узла СПД, в центре которого находится коммутатор K_1, который соединен дуплексными каналами с другими магистральными коммутаторами (K_2 и другими). В качестве его нагрузки выступают коммутаторы, образующие сегменты корпоративных ЛВС, маршрутизаторы, серверы. Разделяемыми ресурсами являются доступ к серверам и доступ к магистрали. Если все пользователи СПD и ЛВС по каналам 100 Мбит/с будут обращаться к серверам, подключенным к коммутатору на такой же скорости, то в этих сегментах велика вероятность возникновения перегрузки. Следовательно, скорость передачи в каналах, ведущих к общим ресурсам, должна быть примерно на порядок больше.

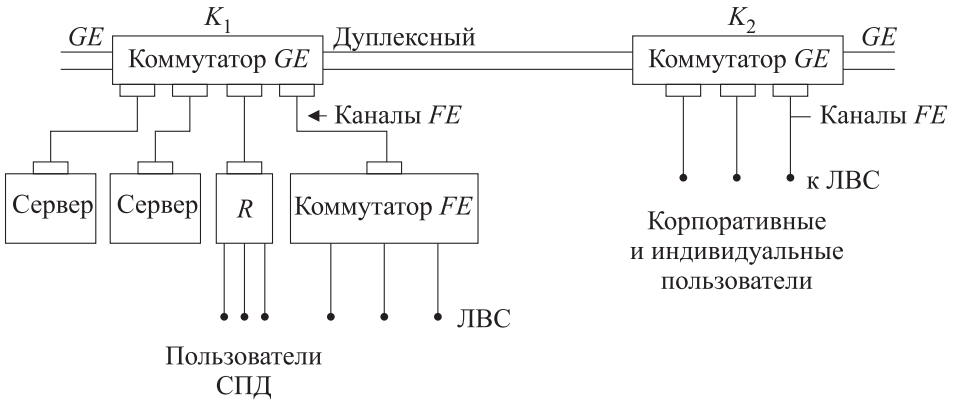


Рис. 2.26 – Фрагмент сети передачи данных

Разработчикам сетевых технологий было предложено несколько разновидностей скоростных сетей: *Asynchronous Transfer Mode (ATM), Fibre Channel (FC), Dynamic Packet Transport (DPT), Gigabit Ethernet*. Рассмотрим здесь последнюю, поскольку она логически вытекает из цепочки технологий *Ethernet* → *Fast Ethernet*, не требует радикальной реконструкции существующих сетей и находит широкое применение. Комитетом IEEE 802.3 приняты стандарты 802.3z и 802.3ab, регламентирующие несколько вариантов сетей *Gigabit Ethernet* с пропускной способностью 1000 Мбит/с.

Что осталось в новой технологии от ее предшественников? Это неизменность второго уровня — подуровней *MAC* и *LLC*. Это означает, что сохранился полудуплексный режим доступа *CSMA/CD*. Он, правда, применим для небольших рабочих групп и небольших расстояний (до 100 м). Вместе с тем широко применяется режим *full duplex* (коммутируемый *GE*), который обеспечивает скоростные связи между достаточно удаленными узлами (5 км и более).

Сохранились форматы кадров *Ethernet*, несмотря на их явные недостатки: отсутствие поля приоритетов, наличие кадров переменной длины, невозможность работы в петлевых схемах, невозможность тестирования работоспособности узлов. Именно это обстоятельство обеспечивает эволюционное развитие сетей *Ethernet*.

Наконец, сохранились все виды физических сред первого уровня: ВОЛС, витая пара UTP-5 и коаксиальный кабель (рис. 2.27).

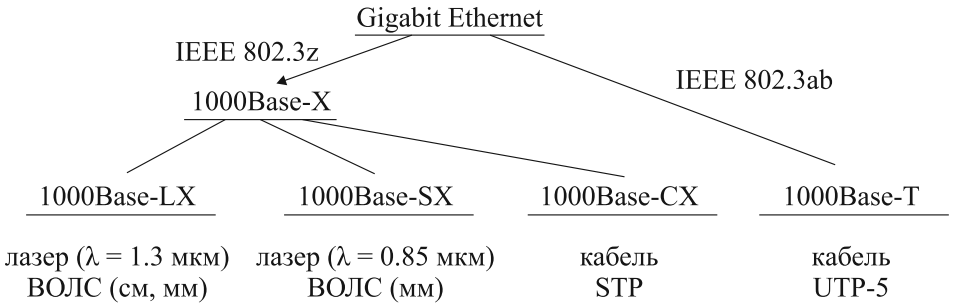
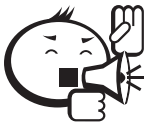


Рис. 2.27 – Физические интерфейсы *Gigabit Ethernet*



Таким образом, все отличия *Gigabit Ethernet* в основном проявляются на физическом уровне.

Они состоят в наличии различных вариантов подключения станций и узлов к сети.

В *1000Base-X* за основу взяты элементы стандарта *Fibre Channel* (*FC*) — технологии взаимодействия быстродействующих рабочих станций и узлов локальных сетей по оптоволокну. Для логического кодирования применен код 8B/10B, аналогичный коду 4B/5B, описанному в разделе 2.8. Этот код по сравнению с 4B/5B практически не содержит постоянной составляющей, что исключает перегрузку лазерных диодов.

1000Base-X в свою очередь разделен на три интерфейса.

1000Base-SX работает с коротковолновыми лазерами (λ = 0.85 мкм) и многомодовом волокном. Достоинством работы в этом диапазоне является то, что источники излучения (лазерные диоды и светодиоды) намного дешевле, а недостатком — большое затухание оптического излучения в волокне. Поэтому предельная длина оптоволоконного сегмента ограничена (табл. 2.8) сотнями метров даже в дуплексном режиме.

1000Base-LX разрешает работу с одномодовым волокном, где характеристики и по затуханию и дисперсии значительно лучше. Потому длина сегментов может составлять несколько километров. Этот стандарт допускает также работу и с многомодовым волокном. Однако в этом случае выигрыш в длине сегмента по сравнению с *1000Base-SX* не такой значительный.

1000Base-CX — этот интерфейс предназначен для работы на экранированной витой паре. Если в кабеле две пары (твинаксиальный кабель), то обе одновременно используются для передачи пакетов в одну сторону и режим сети — полудуплексный. Для полнодуплексного режима применяется *Quad*-кабель, имеющий четыре пары. Максимальная длина сегмента составляет всего 25 м, поэтому этот стандарт применяется для оборудования, расположенного в одной комнате.

1000Base-T — этот стандарт разработан специально для электрического кабеля *UTP*-5, широко применяемого в ЛВС и, в том числе, в технологии *Fast Ethernet*. Для того чтобы обеспечить скорость передачи в дуплексном режиме 1000 Мбит/с, были предложены следующие технические решения:

1. Передача и прием параллельно по всем четырем парам сразу. Поэтому скорость в каждой паре будет уже 250 Мбит/с.

2. Применено многоуровневое кодирование PAM-5 с числом уровней 5 (0, ±1, ±2). При этом за каждый бод (один импульс) передается два бита — комбинации 00, 01, 10, 11. Таким образом, тактовая частота и ширина спектра сигнала составляют 125 МГц. Эти характеристики сигнала позволяют пропускать его через кабель *UTP*-5 без заметного ухудшения пропускной способности.

Код PAM-5 имеет избыточность, так как пять уровней могли бы передавать 2.32 бита за одну посылку. Эта избыточность используется для повышения помехоустойчивости. Появление запрещенных комбинаций сигнализирует об искажении сигнала помехами.

3. Для обеспечения разделения передаваемого и принимаемого сигналов применяются гибридные мостовые устройства.

4. Для отделения принимаемого сигнала от сигнала собственного передатчика, проникающего на вход приемника через мостовую схему, применяется сигнальный процессор, который из смеси вычитает сигнал передатчика.

Все эти меры позволяют реализовать длину сегмента *1000Base-T* до 100 м.

Рассмотренные выше ограничения максимального сегмента сети обусловлены, в первую очередь, затуханием сигнала в кабеле. В полудуплексном режиме необходимо также учитывать влияние коллизий. При сокращении длительности битового интервала BT до 1 нсек соответственно в 10 раз уменьшится и PDV, и максимальный диаметр сети, который будет равен 25 м. Чтобы сохранить диаметр сети в 200 м, необходимо увеличить минимальный размер кадра. Поэтому в *Gigabit Ethernet* он составляет 512 байт вместо 64 байт. Вместе с задержкой в концентраторе это позволяет уложиться в 200 м.

Таблица 2.8 – Стандарты 1000Base-X

Стандарт	**Тип волокна/медного кабеля**	**Полоса пропускания, МГц × км**	**Максимальное расстояние, м**
1000*Base-LX*	Одномодовое волокно (9 мкм)	—	> 5000
	Многомодовое волокно (50 мкм)	500	550
	Многомодовое волокно (62.5 мкм)	320	400
1000*Base-SX*	Многомодовое волокно (50 мкм)	400	500
	Многомодовое волокно (62.5 мкм)	160	220
1000*Base-CX*	Экранированная витая пара STP 1500 м	—	25

При передаче коротких кадров (< 512 байт) применяются следующие приемы.

1. Короткий кадр расширяется так, чтобы поле данных составляло 448 байт. Это заполнение производится запрещенными комбинациями кода 8B/10B, которые после приема кадра удаляются.

2. Одна станция может передавать подряд несколько коротких кадров. Общая длина посылки не должна превышать 8192 байта. Такой режим носит название *Burst Mode* — монопольный пакетный режим. Поскольку скорость передачи высока (1000 Мбит/с), то увеличение длительности передачи практически не задерживает доступ к среде передачи других станций.

Основными устройствами сетей *Gigabit Ethernet* являются:

1. Сетевая карта.

Сетевые карты работают с высокоскоростными шинами *PCI*, обеспечивают скорость передачи в несколько гигабит в секунду. Имеют два независимых процессора в составе приемника и передатчика. Поддерживают стандарты *IEEE* 802.3*x*, *IEEE* 802.3*z*, *IEEE* 802.*ab*, что делает их практически совместимыми со всеми другими устройствами.

2. Концентратор (буферный повторитель).

Существенным отличием буферного повторителя является то, что он по каждому входному и выходному портам имеет устройства памяти. Поскольку сетевые станции также имеют независимые порты передатчика и приемника, то на участке станция — буфер повторителя реализуется дуплексный режим. На этом участке механизм CSMA/CD исключен и коллизий нет. Внутри повторителя реализуется алгоритм случайного доступа CSMA/CD, когда пакеты из входного буфера принимающего порта передатчика передаются на выходные буферы остальных портов. Таким образом, ограничения на длину сегмента, связанные с коллизиями, здесь не работают. Остаются только ограничения, связанные с физическими характеристиками линий (затухание, дисперсия). Поэтому применение волоконно-оптических кабелей в сетях Gigabit Ethernet предпочтительней.

3. Коммутатор.

Осуществляя функции объединения сетей, коммутаторы Gigabit Ethernet имеют порты всех трех уровней: GE, FE и Ethernet. Так, число портов 1000Base-SX/LX в одном модуле может меняться от 2 до 16. При этом число портов 10/100Base-TX может достигать 48. Общее число модулей до 10. Возможен выбор физического интерфейса.

При необходимости порты GE и FE могут объединяться с целью увеличения пропускной способности до 8–16 Гбит/с. Для обеспечения таких скоростей шина коммутатора работает с пропускной способностью 24–156 Гбит/с.

Для контроля и управления потоком коммутаторы поддерживают стандарт IEEE 802.3x. Этот стандарт при перегрузке реализует команду «Приостановить передачу», которая передается соседнему узлу с помощью выбранных избыточных символов кода 8B/10B. После снятия перегрузки аналогично передается команда «Возобновить передачу».

Кроме этих функций, коммутаторы реализуют:

- поддержку механизма QoS протокола RsVP (Resource Reservation Protocol);
- поддержку различных протоколов для организации виртуальных сетей (VTP, IEEE 802.1Q и др.);
- горячее резервирование электропитания и управления;
- возможность дистанционного управления.

2.10 10 Gigabit Ethernet (10GE)

Достоинство технологии Ethernet позволило обеспечить дальнейшее наращивание скорости передачи данных. Вслед за Gigabit Ethernet появились технологии 10 Gigabit Ethernet (10GE) и 100 Gigabit Ethernet (100GE) со скоростями передачи 10 Гбит/с и 100 Гбит/с соответственно.

Рассмотрим здесь технологию 10GE подробнее.

Технология 10GE стандарт IEEE 802.3ae в отличие от Gigabit Ethernet используется только в режиме коммутации (*full duplex*). Режим общей разделяемой среды (технология с использованием хабов) не применяется в связи с тем, что размер домена коллизий сокращается до нескольких метров. Формат кадра остается такой же, как в классическом Ethernet. Существуют три группы таких физических интерфейсов: 10GBase-X, 10GBase-R и 10GBase-W. Они отличаются тем, что в технологии 10GBase-X для увеличения пропускной способности используется метод спектрального уплотнения WDM, в рамках которого передаются пакеты без преобразования их в стандартную форму SDH. В технологиях 10GBase-R и 10GBase-W информация сетей передачи данных инкапсулируется в кадры STM 64. Кроме этого, они отличаются способом кодирования данных: в варианте 10Base-X применяется код 8B/10B, в остальных двух — код 64B/66B. Все они для передачи данных задействуют оптическую среду.

Группа 10GBase-X в настоящее время состоит из одного интерфейса 10GBase-LX4. Буква L говорит о том, что информация передается с помощью волн второго диапазона прозрачности, то есть 1310 нм. Информация в каждом направлении передается одновременно с помощью четырех волн (что отражает цифра 4 в названии интерфейса), которые мультиплексируются на основе техники WDM (см. раздел 3.1). Каждый из четырех потоков интерфейса XGMII передается в оптическом волокне со скоростью 2.5 Гбит/с. Максимальное расстояние между передатчиком и приемником стандарта 10GBase-LX4 на многомодовом волокне равно 200–300 м (в зависимости от полосы пропускания волокна), на одномодовом — 10 км.

Интерфейсы 10GBase-W и 10GBase-R используют технологию SDH. В отличие от 10GBase-X эта технология является наложенной, когда пакеты Ethernet размещаются в кадрах синхронного транспортного модуля STM-64 (скорость 10 Гбит/с). В каждой из групп 10GBase-W и 10GBase-R может быть три варианта подуровня PMD: S, L и E в зависимости от используемого для передачи информации диапазона волн — 850, 1310 или 1550 нм соответственно. Таким образом, существуют интерфейсы 10GBase-WS, 10GBase-WL, 10GBase-WE и 10GBase-RS, 10GBase-RL и lOGBase-RE. Каждый из них передает информацию с помощью одной волны соответствующего диапазона.

Пропускная способность интерфейсов группы W равна 9.95328 Гбит/с, а эффективная скорость передачи данных — 9.58464 Гбит/с (часть пропускной способности тратится на заголовки кадров STM). Из-за того что скорость передачи информации у этой группы интерфейсов ниже, чем 10 Гбит/с, они могут взаимодействовать только между собой, то есть соединение, например интерфейсов 10GBase-RL и 10Base-WL, невозможно. Интерфейсы группы W не являются полностью совместимыми по электрическим характеристикам с интерфейсами SDH STM-64. Поэтому для соединения сетей 10G Ethernet через первичную сеть SDH у мульти-

плексоров первичной сети должны быть специальные 10-гигабитные интерфейсы, совместимые со спецификациями 10GBase-W. Поддержка оборудованием 10GBase-W скорости 9.95328 Гбит/с обеспечивает принципиальную возможность передачи трафика 10G Ethernet через сети SDH в кадрах STM-64.

Контрольные вопросы по главе 2

1. Чем отличаются подуровни MAC и LLC?
2. Объясните причину того, что MAC-адреса не обладают иерархичностью.
3. В чем заключается разница между технологиями CSMA/CD и CSMA/CI?
4. Опишите манчестерский код.
5. Назовите основные достоинства технологии «Коммутируемый Ethernet».
6. Какая среда передачи используется в протоколах Gigabit Ethernet и 10 Gigabit Ethernet?

Глава 3

ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ СЕТЕЙ

3.1 Общие понятия и принципы

Под глобальными вычислительными сетями (ГВС) будем понимать сети, охватывающие значительные территории: регион, страна, значительная часть земного шара [1, 2, 4]. Примерами ГВС можно считать, например, сеть ОАО «Транстелеком», которая охватывает все железные дороги России и, наконец, всемирную сеть Интернет.

Отличительными особенностями глобальных сетей являются:

- большие расстояния между узлами и станциями;
- большие задержки сигнала;
- более равномерный трафик, что обусловлено большим количеством независимых пользователей;
- более сложные процедуры передачи, что связано с меньшей надежностью;
- обязательное использование технологий сетевого уровня ЭМВОС.

Известными технологиями ГВС являются: Frame Relay (FR), IP (Internet Protocol), ATM, NGN. Доминирующей сетевой технологией на данный момент является IP. Она начинает работать только с третьего уровня и подробно будет рассмотрена в следующих разделах. Здесь же мы дадим характеристику и подробней опишем основные протоколы первого и второго уровней.

На физическом уровне в сетях большого масштаба наибольшее распространение получили технологии цифровых систем передачи PDH и SDH, которые организуются либо по волоконно-оптическим линиям связи, либо по РРЛ. В зависимости от требуемых объемов трафика и скорости передачи для абонентов ГВС выделяются необходимые цифровые каналы до $n \times 155$ Мбит/с. Пакеты абонентов размещаются в цифровых каналах с помощью мультиплексоров и передаются в общем цифровом потоке вместе с другими видами нагрузки (телефония, сотовая связь, видеоинформация). Такие сети, в которых трафик передачи данных размещается в общем цифровом потоке, называются наложенными.

Наряду с этим применяются и выделенные сети, в которых передается только трафик передачи данных. Технологиями физического уровня здесь, «как правило», являются Fast Ethernet, Gigabit Ethernet, 10 Gb Ethernet, описанные в предыдущем разделе.

Наряду с этими технологиями в глобальных сетях также широко применяются классические методы цифровых систем передачи (PDH, SDH, WDM). Рассмотрим здесь подробней технологию спектрального уплотнения WDM (Wavelength Division Multiplexing). Системы с WDM относятся к системам с частотным разделением каналов (ЧРК). Отличие от классических систем с ЧРК заключается в том, что различные оптические несущие (лазеры, излучающие на разных длинах волн) модулируются по интенсивности цифровыми импульсными сигналами от различных источников информации. Затем лазерные лучи объединяются в один световой поток в оптическом мультиплексоре. Расстояния между оптическими несущими должны быть такими, чтобы не создавать заметных перекрестных искажений.

Основная схема системы с WDM (для примера взято четыре канала) имеет вид, представленный на рисунке 3.1 (показан один прямой канал).

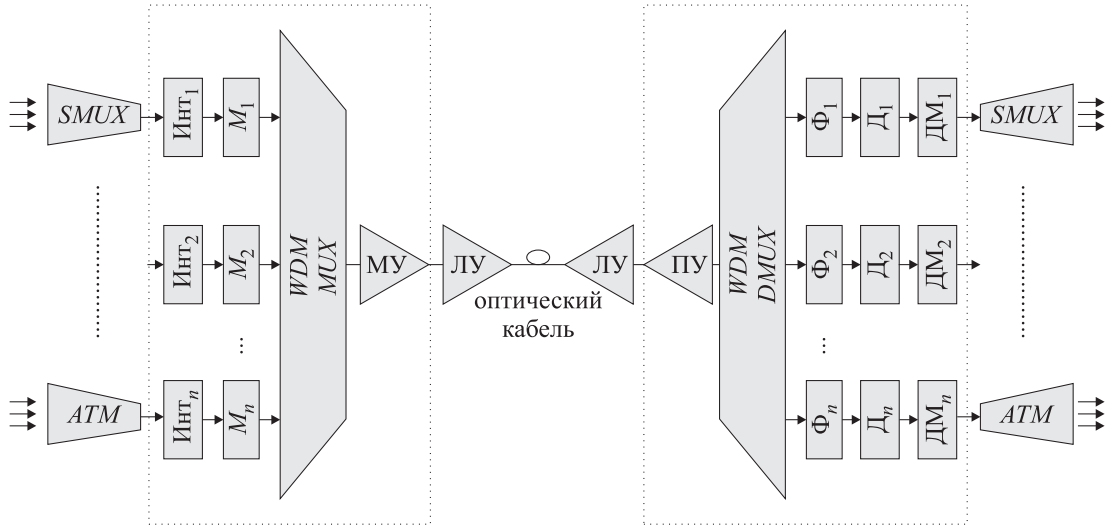


Рис. 3.1 – Схема системы с WDM

Здесь n входных потоков данных (кодированных цифровых импульсных последовательностей) модулируют (модуляция основной полосой) с помощью оптических модуляторов M_i оптические несущие с длинами волн l_i. Модулированные несущие мультиплексируются (объединяются) с помощью мультиплексора WDM

MUX в агрегатный поток, который после усиления (с помощью бустера или мощного усилителя — МУ) подается в оптический кабель (ОК). На приемном конце поток с выхода ОК усиливается предварительным усилителем — ПУ, демультиплексируется, т. е. разделяется на составляющие потоки — модулированные несущие l_i, которые детектируются с помощью детекторов $Д_i$ (на входе которых могут дополнительно использоваться полосовые фильтры $Ф_i$ для уменьшения переходных помех и увеличения тем самым помехоустойчивости детектирования), и, наконец, демодулируются демодуляторами $ДМ_i$, формирующими на выходе исходные кодированные цифровые импульсные последовательности. Кроме МУ и ПУ, в системе могут быть использованы и линейные усилители — ЛУ (как рассматривалось выше).

Самым первым и наиболее простым вариантом WDM является такой, когда в одном волокне одновременно передаются два цифровых потока в окнах прозрачности с длинами волн 1310 нм и 1550 нм. В этом случае пропускная способность линии увеличивается в два раза, а перекрестные помехи практически равны нулю.

Дальнейшее наращивание пропускной способности реализуется в системах, у которых число оптических несущих равно 4 и более.

Их можно классифицировать следующим образом:

- WDM — системы с частотным разносом каналов не менее 200 ГГц, позволяющие мультиплексировать не более 16 каналов;
- DWDM — системы с разносом каналов не менее 100 ГГц, позволяющие мультиплексировать не более 64 каналов;
- HDWDM — системы с разносом каналов 50 ГГц и менее, позволяющие мультиплексировать не менее 64 каналов.

Первые мультиплексоры класса WDM использовались для мультиплексирования двух несущих: 1310 нм и 1550 нм, расстояние между которыми 240 нм было настолько большим, что при реализации не требовало специальных фильтров для их разделения. Дальнейшие усилия, направленные на улучшение селективности (уменьшение разноса каналов), при использовании традиционной дискретной оптики не давали результатов лучше, чем следующие:

- разнос каналов — 20–30 нм;
- переходное затухание между каналами — 20 дБ;
- уровень вносимых потерь — 2–4 дБ.

Это позволило формировать не более 4 каналов во 2-м окне прозрачности. Затем произошел существенный прорыв в технологии мультиплексирования, обусловленный, с одной стороны, переходом к интегральным оптическим технологиям, с другой — миниатюризацией и улучшением качества изготовления элементов традиционной дискретной оптики.

В настоящее время используются три конкурирующие технологии выделения каналов (демультиплексирования). Две из них на основе интегральной оптики: одна использует выделение несущих на основе дифракционной решетки на массиве волноводов — AWG (Arrayed Waveguide Grating) и вторая на основе вогнутой дифракционной решетки — CG (Concave Grating). В третьей технологии применяется традиционная миниатюрная (на новом уровне технологии) дискретная оптика, ис-

пользующая выделение каналов на основе интерферометрических методов — 3DO (3-D Optics WDM). Параметры мультиплексоров WDM, реализованных на основе указанных технологий, сведены в таблицу 3.1.

Таблица 3.1 – Параметры мультиплексоров WDM

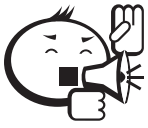
Технология	I/O AWG	I/O CG	3-D Optics WDM
Максимальное число каналов [нм]	32	78	262
Разнос каналов	0.1–15	1–4	0.4–250
Вносимые потери [дБ]	6–8	10–16	2–6
Переходное затухание [дБ]	−5 — −29	−7 — −30	−30 — −55
Чувствительность к поляризации, %	2	2–50	0

Из таблицы видно, что технология 3-D Optics WDM имеет преимущество по четырем из пяти параметров и может быть использована в системах WDM до уровня HDWDM с разносом каналов не меньше 0.4 нм.

3.2 Реализация функций канального уровня в глобальных сетях

Канальный уровень обеспечивает надежную передачу данных через физический канал (между двумя точками) и в том числе:

- адресацию передаваемых сообщений;
- прием и передачу данных;
- формирование кадров;
- выявление неисправностей и ошибок;
- управление потоком информации.



В глобальных сетях на канальном уровне используются протоколы «точка — точка»:

- SLIP — Serial Line Internet Protocol,
- HDLC — High Level Data Link Control — семейство протоколов,
- PPP — Point to Point Protocol,
- Ethernet.

Особенностью протоколов является необходимость управления потоком, поскольку в канале передачи могут находиться промежуточные узлы с буферными устройствами, которые могут переполняться.

3.2.1 Протокол SLIP

Это первый и наиболее простой протокол канального уровня и применяется только для передачи пакетов TCP/IP. К его достоинствам помимо простоты относится возможность подключения через интерфейс RS-232, а к недостаткам:

- отсутствие механизма адресации;
- невозможность идентификации протоколов сетевого уровня;
- отсутствие механизма определения и коррекции ошибок.

Структура пакета SLIP вместе с пакетом IP приведена на рисунке 3.2. Здесь формирование пакета происходит оконечиванием IP-пакета специальными символами END. Значение END в шестнадцатеричном представлении равно CO. Если в передаваемом сообщении случайным образом возникает комбинация CO, то она заменяется другой DB-DC, а если встретится DB, то замена DB-DD.

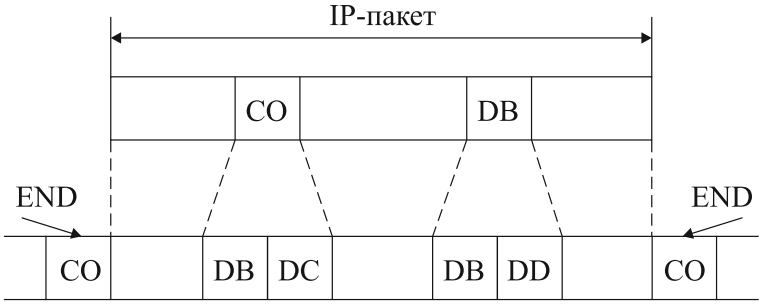


Рис. 3.2 – Формирование SLIP-пакета

В спецификации протокола SLIP не определена максимальная длина IP-пакета, но реально он не может быть более 1000 байт вместо допускаемых IP-протоколом 1500 байт. Для установления связи по протоколу SLIP станции должны иметь информацию об IP-адресах друг друга. Поэтому передача пакета через промежуточные маршрутизаторы невозможна.

3.2.2 Протоколы HDLC

В семейство протоколов HDLC входят много известных протоколов: LAP-B (канальный уровень стека X.25), LAP-D (уровень обмена сигнальной информации ISDN), LAP-F (Frame Relay) и др.

Основные механизмы протокола HDLC:

- установление логического соединения;
- наличие различных типов кадров (информационных и служебных нумерованных и ненумерованных);
- анализ битовых последовательностей для проведения процедур выявления ошибок;
- управление потоком с помощью метода «скользящего окна» (рис. 3.3).

Суть метода «скользящего окна» заключается в следующем. Окно — это непрерывный диапазон *n* кадров, которые могут находиться в канале передачи одновременно. При передаче кадры отправляются, и передатчик ждет подтверждения.

Только после подтверждения о приеме первого кадра передатчик отправляет в канал кадр с номером $n + 1$.

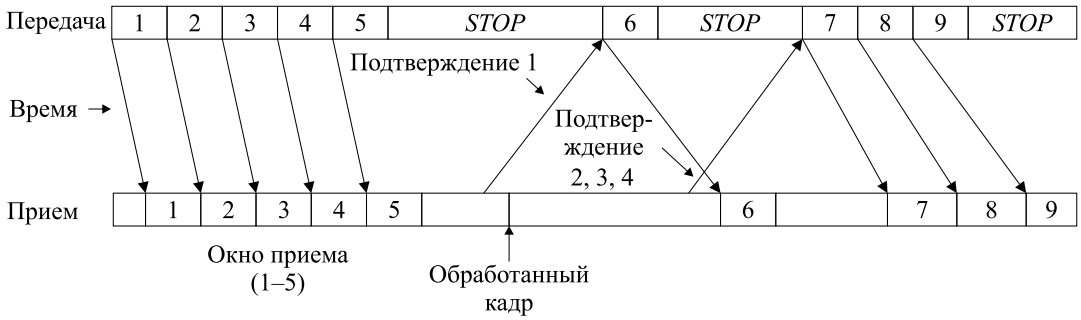
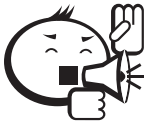


Рис. 3.3 – Иллюстрация метода скользящего окна

Окна страхуют буферы приемника и передатчика от переполнения. Если буфер приемника заполнен, то он не посылает подтверждения. Также устанавливаются и искаженные и потерянные кадры, которые потом передаются повторно. Окно называется скользящим потому, что его размер переменный и составляет обычно от 1 до 7 кадров.

3.3 PPP-протокол

Основой этого протокола также является HDLC, но он с одной стороны существенно упрощен, а с другой допускает перенос пакетов различный сетевых протоколов в одном логическом канале связи. PPP разработан взамен устаревшего SLIP и в настоящее время является практически основным протоколом канального уровня для глобальных связей при удаленных соединениях. При этом при установлении соединения вначале осуществляется переговорный процесс по согласованию параметров соединения (качество линии, протоколы аутентификации и сетевого уровня).



Протокол PPP состоит из двух компонент:

- LCP — Link Control Protocol — протокол управления связью, которым согласуются параметры соединения;
- NCP — Network Control Protocol — протокол управления сетевым уровнем, которым согласуется протокол третьего уровня, например IP или IPX.

Базовый формат кадра PPP приведен на рисунке 3.4. Здесь флаг 7 E = 01111110 определяет начало и конец кадра, а также задает тактовую синхронизацию. Поле адреса всегда занято одной и той же последовательностью FF = 11111111, потому что это поле унаследовано из формата HDLC и в режиме «точка — точка» адресация не нужна. В то же время последовательность «единиц» обеспечивает надежную синхронизацию.

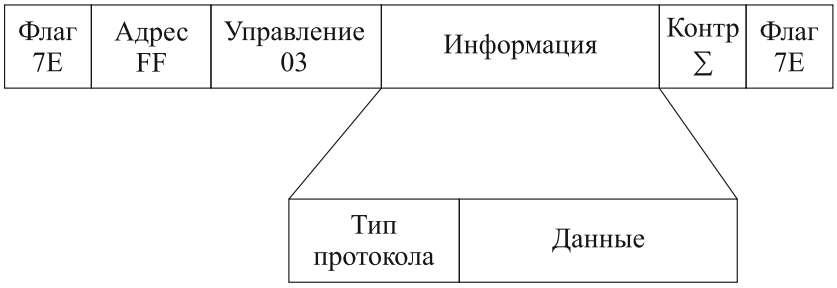


Рис. 3.4 – Формат кадра PPP

Поле управления также всегда постоянно (03), что в терминах HDLC означает, что все кадры PPP — информационные и ненумерованные, т. е. при потере кадра на канальном уровне они не восстанавливаются. Поле контрольной суммы размером 16 или 32 бит задает стандартную процедуру обнаружения ошибок с помощью циклических кодов с полиномом типа: $x^{16} + x^{12} + x^5 + 1$.

Наконец, поле «информация» несет основную смысловую нагрузку как при переговорных процессах, так при передаче пакетов с данными. В этом поле указывается тип работающего в данный момент протокола и передаваемая с ним информация. Документ RFC 1700 определяет следующие возможные значения этого поля:

- С xxx — LCP сообщение,
- 8 xxx — NCP сообщение,
- О xxx — сообщение верхнего (сетевого) уровня.

Сами сообщения заключены в поле «Данные».

Рассмотрим фазы работы протокола PPP. Их четыре: три обязательные и одна необязательная.

1. Фаза установления соединения (LCP) содержит команду запроса «Configure Request» от передатчика к приемнику и ответ «Configure Ask». В случае положительного ответа, когда все параметры канала согласованы, он открыт.
2. Фаза аутентификации по протоколам PAP — Password Authentication Protocol или CHAP — Challenge Handshake Authentication Protocol. Эта фаза необязательна. Она проходит в обе стороны по командам PAP или CHAP. Если аутентификация состоялась, то канал переходит к следующей сетевой фазе, если нет, то к завершающей фазе.
3. Сетевая фаза (NCP). Эта фаза содержит следующие процедуры:

   3.1 Открытие сессии одного из протоколов сетевого уровня, например IP, по командам:

   - Configure Request (IP) — от передатчика;
   - Configure Ask (IP) — от приемника;
   - Configure Request IP Adress — запрос IP-адреса;
   - Configure Request IP Adress — ответ;
   - Data Exchange — обмен данными в обе стороны.

4. Фаза завершения (LCP). Эта фаза обязательна, и она состоится не только после окончания сеанса, но и в случаях физического сбоя в канале, плохого качества передачи, отсутствия аутентификации, по воле администратора сети, по командам:
   - Terminate request,
   - Terminate Ask.

Рассмотрим теперь структуру поля «информация» (рис. 3.4) для пакетов LCP (рис. 3.5). Здесь после кода LCP пакета (С xxx) идет код сообщения:

1. Configure Request (код = 1). Как уже говорилось, сообщением с кодом = 1 открывается соединение, состоится обмен параметрами канала и прием согласованных параметров с противоположной стороны.
2. Configure Ask (код = 2). Здесь передается ответ на запрос Configure Request и подтверждается правильность предлагаемых параметров. По прибытии этого пакета канал должен быть открыт.
3. Configure Nak (код = 3). Передача этого кода означает, что значения параметров неприемлемы.
4. Configure Reject (код = 4). Этим кодом сообщается, что некоторые из параметров некорректны, и посылается новый пакет Configure Request без этих параметров.

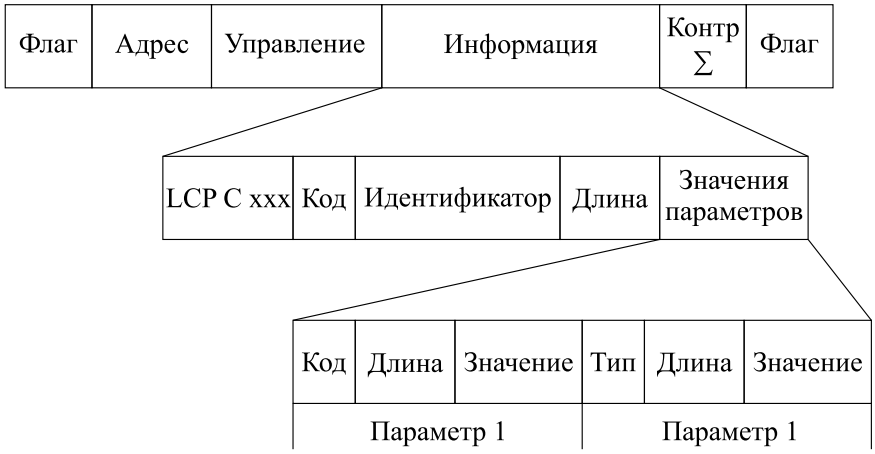


Рис. 3.5 – Передача информации о параметрах канала в сессии LCP

Следующее поле в пакете LCP — идентификатор. Здесь LCP-запросы и соответствующие LCP-ответы отмечаются одним и тем же номером. Поле «Длина» указывает размер LCP-пакета.

Непосредственная информация о параметрах содержится в поле «Значение», которое в свою очередь делится на три раздела: «Тип» — описывает назначение и номер параметра, «Длина» — задает размер значения параметра и «Значение» — само значение параметра. Всего параметров 8. Основные из них: максимальный размер пакета, протокол аутентификации (PAP или CHAP), длина поля контрольной суммы, протокол оценки качества.

Точно такая же процедура производится и во время фазы NCP. Здесь в поле «Информация» в первую очередь согласуется тип сетевого протокола 8 xxx.

Для протокола IP 8 xxx = 8021, а согласуемыми параметрами являются IP-адрес получателя сообщения и алгоритм сжатия. Для этого используется алгоритм Ван Якобсена, когда заголовки IP и TCP уменьшаются от 40 байт и более до 3–5 байт.

В протоколе PPP есть также механизмы для постоянного слежения за качеством передачи. Эта процедура Link Quality Report (LQR), которая подсчитывает долю успешно переданных пакетов. Если эта доля меньше установленного порога, сессия NCP закрывается. Во второй процедуре Echo Request качество линии определяется с помощью специальных тестов.

В настоящее время доминирующим протоколом канального уровня в ГВС является Ethernet (GE, 10GE, 100GE). Основная функция канального уровня (адресация) реализуется с помощью коммутаторов и MAC-адресов (см. раздел 2).

Контрольные вопросы по главе 3

1. На каких уровнях семиуровневой модели взаимодействия открытых систем работают глобальные сети?
2. Опишите суть и фазы работы протокола PPP.
3. В чем заключается суть технологии «скользящего окна»?
4. Какие технологии физического уровня применяются в глобальных сетях?
5. Какая основная технология канального уровня применяется в глобальных сетях?

Глава 4

IP-СЕТИ

4.1 Общие положения

Рассмотренные ранее технологии (Ethernet, FE, GE, PPP, HDLC) не могут претендовать на роль технологии глобальных вычислительных сетей, поскольку все они работают на втором (канальном) уровне ЭМВОС. Это означает, что если сеть сложная и содержит большое количество узлов, то пакеты данных сами не смогут проложить себе маршрут следования от узла к узлу. MAC-адреса и таблицы коммутаторов с такой задачей не справляются, так как они не обладают свойством иерархичности. В таблицах коммутаторов должны содержаться адреса всех станций. К другим недостаткам сетей на основе коммутаторов относятся:

- невозможность построения кольцевых и ячеистых схем, что исключает возможность резервирования и регулирования нагрузки;
- перегрузки сетей при широковещательных рассылках информации (широковещательные штормы);
- невозможность взаимодействия сетей, работающих на разных протоколах канального уровня.

Таким образом, при построении больших сетей необходимы новые, более интеллектуальные принципы организации сетей. Эти принципы определяются третьим (сетевым) и четвертым (транспортным) уровнями:

1. Сети работают по технологиям коммутации пакетов, причем допускаются режимы:
   - без установления соединений (датаграммный);
   - с установлением соединения (метод виртуального соединения).
2. Сеть должна быть иерархична, т. е. система адресации должна содержать высшие разряды для узлов верхнего порядка (крупные провайдеры) и низшие разряды для узлов нижнего уровня и отдельных пользователей.

3. Сеть должна быть открытой, т. е. доступной для любого пользователя, а не только для корпоративных клиентов.
4. Сеть должна быть в состоянии объединять ЛВС или корпоративные сети, работающие по разным протоколам канального и сетевого уровней.
5. Сеть должна выбирать для пакетов оптимальный маршрут по некоторому критерию и передавать пакеты по этому маршруту.

К известным технологиям сетевого уровня относятся: IP, IPX (Novell), X.25 (IEEE), Frame Relay, ATM [1, 11, 12]. Доминирующим способом передачи на сегодняшний день является IP, поскольку он удовлетворяет практически всем перечисленным выше условиям. Протоколы IP и работающие над ним TCP и UDP и будут рассмотрены в этом разделе. Что касается других технологий, то они вытесняются TCP/IP по разным причинам.

Технология X.25, предложенная IEEE, разрабатывалась в условиях, когда на сетях связи преобладали линии с низким качеством и обеспечить вероятность ошибки $P_{ош} \approx 10^{-8}$ можно было только с помощью сложной и длительной процедуры решающей обратной связи, когда информация о прохождении пакета на каждом этапе подтверждалась. При отсутствии подтверждения передача повторялась. Здесь также предварительно устанавливалось виртуальное соединение. Эти и другие процедуры требовали большого времени, поэтому скорость передачи по протоколу X.25 составляла десятки килобит в секунду. В настоящее время технология X.25, являющаяся, прежде всего, закрытой, корпоративной, практически не применяется.

Технология Frame Relay (FR) является скорректированным вариантом X.25. Коррекция проведена в связи с улучшением качества передачи в линиях связи, поэтому квитирование передачи пакетов между узлами отменено. Оно оставлено только для последней (приемной) станции. При этом все сомнительные пакеты просто отбрасываются. Эти упрощения позволяют обеспечить скорость передачи до 2 Мбит/с.

Особенностью технологии FR является гарантированная поддержка основных показателей качества передачи — средней скорости передачи по виртуальному каналу при допустимых уровнях пульсации трафика.

Основной областью применения FR остается построение корпоративных сетей путем объединения удаленных друг от друга ЛВС. При большом количестве точек доступа число виртуальных каналов становится недопустимо большим, что указывает на невозможность построения глобальных сетей.

Технология ATM — самая молодая из перечисленных выше. Она задумывалась как универсальная мультисервисная технология для передачи данных, речи и видео. Подходит она и для построения глобальных вычислительных сетей, поскольку пакеты ATM могут передаваться поверх SDH. Вместе с тем необходимость учета многих противоречивых требований в мультисервисных сетях привела к существенному удорожанию оборудования по сравнению с другими технологиями, что сдерживает широкое применение ATM.

Протоколы IP и IPX достаточно похожи, но технология IPX фирмы Novell разрабатывалась для ЛВС, в то время как IP — для глобальных сетей. В IP и IPX сетевой адрес делится на номер сети и номер узла, что обеспечивает необходимую иерархичность. Однако в IPX номер узла привязан к MAC-адресу ЛВС, и это

серьезное ограничение для больших сетей. В IP этого ограничения нет, так как номер узла определяется числом, подчиняющимся законам иерархии и никак не связанным с MAC-адресом.

Стек протоколов TCP/IP разрабатывался для сколь угодно больших сетей с высокой надежностью функционирования. В этой технологии предполагается большое количество резервных путей между любыми двумя узлами и датаграммный способ доставки пакетов (UDP/IP). Структура адресации обеспечивает необходимую иерархичность, что существенно облегчает работу узлов распределения нагрузки (маршрутизаторов). Международная система распределения адресов делает сеть открытой и глобальной в международном масштабе. Наконец, технология IP не зависит от нижних уровней и может работать с технологиями Ethernet, PPP, FR, ISDN и другими. Наряду с датаграммным режимом доставки сочетание протокола IP с протоколом транспортного уровня TCP позволяет реализовать режим виртуального соединения.

Таким образом, технология IP, которая непрерывно совершенствуется, является очень удобной для реализации глобальных сетей и на данный момент доминирующей. Конкуренцию ей составляет ATM.

Прежде чем рассмотреть алгоритм передачи IP-пакетов, установим связь протоколов стека TCP/IP с ЭМВОС (рис. 4.1).

<table>
<tr><td>7
6</td><td colspan="2">WWW, SNMP, FTP, Telnet, SMTP и др.</td><td>Прикладной уровень</td></tr>
<tr><td>5
4</td><td>TCP</td><td>UDP</td><td>Транспортный уровень</td></tr>
<tr><td>3</td><td colspan="2">IP</td><td>Уровень межсетевого взаимодействия</td></tr>
<tr><td>2
1</td><td colspan="2">Ethernet, PPP, SLIP, X.25, FR, ATM</td><td>Уровень сетевых интерфейсов</td></tr>
</table>

Рис. 4.1 – Связь уровней TCP/IP с ЭВМОС

Как видно, модель уровней TCP/IP отличается от ЭВМОС. Эти отличия заключаются как в количестве уровней, так и в их функциональном содержании. Начнем снизу. Первый и второй уровни в стеке протоколов TCP/IP не регламентируются. Это означает, что третий (сетевой) уровень IP должен взаимодействовать с любым протоколом канального уровня. Это взаимодействие, как правило, решается с помощью инкапсуляции IP-пакетов в кадры канального уровня, например Ethernet или PPP (рис. 4.2).

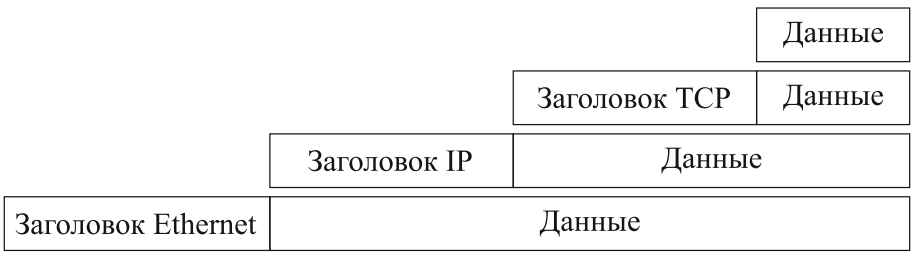
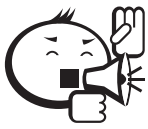
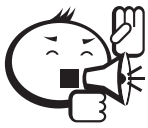


Рис. 4.2 – Инкапсуляция данных различных уровней



Уровень межсетевого взаимодействия IP — Internet Protocol совпадает с сетевым уровнем ЭМВОС, поэтому в дальнейшем будем называть его просто сетевым уровнем. Основное его назначение — выбор маршрута следования пакетов по определенному критерию и передача пакета по этому маршруту в составных сетях независимо от протоколов канального уровня.

При этом условия гарантии доставки пакетов в IP не заложены. IP — это протокол негарантированной доставки пакетов. Сам пакет прокладывает себе путь через цепочку маршрутизаторов, выбирая для данного момента самый благоприятный маршрут.



Транспортный уровень с точки зрения передачи пакетов содержит два альтернативных варианта:

- UDP (User Datagram Protocol) — протокол негарантированной доставки, который обеспечивает передачу пакетов датаграммным способом и по сути является продолжением протокола IP.
- TCP (Transmission Control Protocol) — протокол с управлением передачи, принципиально отличающийся от UDP, поскольку он вначале устанавливает виртуальное соединение между двумя абонентами, а потом по этому пути передает их пакеты наряду с пакетами других абонентов. Связь по TCP — дуплексная и без ошибок. По сути дела протокол TCP позволяет в стеке TCP/IP совмещать две разные технологии: датаграммную и виртуального соединения.

Шестой и седьмой уровни функционально объединены в один прикладной, который представляет все сервисы сети Интернет: электронную почту SMTP, доступ к базам данных WWW, передачу файлов FTP и многое другое. Состав сервисов этого уровня непрерывно расширяется.

В данном разделе мы будем подробно рассматривать IP-сети, т. е. сети, построенные на протоколе сетевого уровня — IP. Рассмотрение начнем с заголовка IP-пакета (рис. 4.3).

Здесь поле «Версия» определяет версию протокола IPv4 или IPv6. Сейчас первая, но готовится переход на вторую. Длина заголовка может быть переменной, и эти данные содержатся в поле «Длина заголовка». Поле «Тип сервиса» (Type of Service — ToS) содержит 8 бит. Из них 3 бита определяют уровень приоритета

(*PR*), биты *D*, *T* и *R* — выбор критерия для установления маршрута: *D* — минимизация задержки, *T* — максимизация пропускной способности, *R* — максимизация надежности доставки. Оставшиеся два бита — резерв. Поле «Общая длина» отражает общую длину пакета. В случае кадров Ethernet это не более 1524 байт. Поле «Идентификатор» задает индивидуальный номер пакета. Если исходный пакет разбивается на фрагменты, то используются поля «флаги» и «смещение фрагмента».

<table>
<tr><td rowspan="2">Версия
4 бита</td><td rowspan="2">Длина
заголовка
4 бита</td><td colspan="5">Тип сервиса
8 бит</td><td colspan="2" rowspan="2">Общая длина
16 бит</td></tr>
<tr><td>PR
3</td><td>D
1</td><td>T
1</td><td>R
1</td><td>2</td></tr>
<tr><td colspan="6" rowspan="2">Идентификация 16 бит</td><td colspan="2">Флаги
3 бита</td><td rowspan="2">Смещение
фрагмента
13 бит</td></tr>
<tr><td></td><td>D</td><td>M</td></tr>
<tr><td colspan="2">Время жизни
8 бит</td><td colspan="2">Протокол верхнего
уровня
8 бит</td><td colspan="4">Контрольная сумма
16 бит</td></tr>
<tr><td colspan="8">IP-адрес отправителя
32 бита</td></tr>
<tr><td colspan="8">IP-адрес получателя
32 бита</td></tr>
<tr><td colspan="5">Опции</td><td colspan="3">Выравнивание</td></tr>
</table>

Рис. 4.3 – Структура заголовка IP-пакета

Важнейшие поля — это адреса отправителя и получателя, тип протокола верхнего уровня и время жизни. Поля адресов одинаковы, содержат 32 бита, в которых есть адрес сети и адрес узла. Эти адреса присутствуют в таблицах маршрутизации, по ним составляется путь следования пакета. Поле «Протокол верхнего уровня» сортирует IP-пакеты для передачи на транспортный уровень. Эта сортировка производится по протоколам TCP, UDP, а также протоколу формирования таблиц OSPF и некоторым другим. Поле «Время жизни» определяет время существования пакета в сети, поскольку оно не может быть бесконечным. Как правило, это время измеряется в «хопах» — числе пройденных маршрутизаторов. Когда время жизни будет исчерпано, пакет уничтожается.

Практика показывает, что IP-заголовок избыточен, поэтому его обычно сжимают.

Рассмотрим теперь основы функционирования IP-сетей (рис. 4.4). Здесь представлен фрагмент сети, содержащий три маршрутизатора M_1–M_3 и семь сетей L_1–L_7, связанных между собой с помощью различных интерфейсов и протоколов физического и канального уровней:

- с пакетной организацией связи Ethernet, Fast Ethernet (FE), Gigabit Ethernet (GE), ATM, V35+PPP;
- на цифровых каналах: SDH, PDH (E1), ISDN BRI.

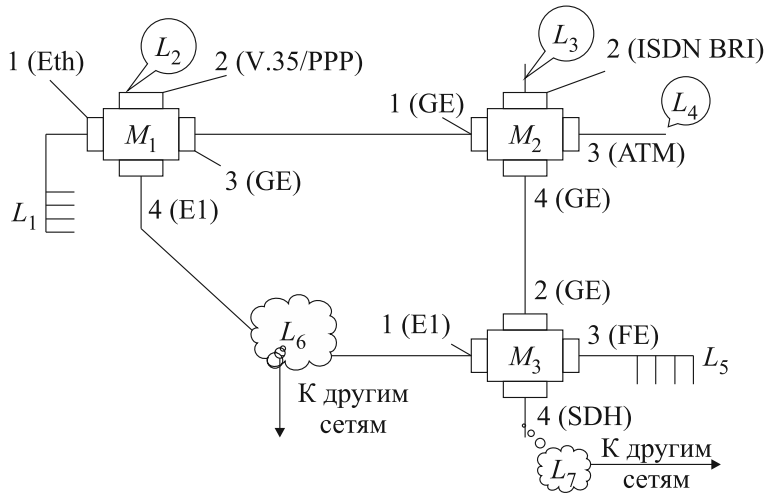


Рис. 4.4 – Фрагмент IP-сети

Маршрутизаторы, следовательно, должны иметь различные порты подключения и уметь работать с соответствующими протоколами второго уровня.

Передача пакетов между сетями производится с помощью маршрутизаторов, которые своими портами подключены к сетям. Например порт 1 маршрутизатора M_1 подключен к сети L_1 и имеет сетевой адрес $M_1(1)$, принадлежащий этой сети. Сам маршрутизатор никаких адресов (IP, MAC) не имеет. Обычно в сложных IP-сетях можно выбрать несколько маршрутов от одной локальной сети к другой. Выбор маршрута и передача пакетов осуществляются с помощью таблиц маршрутизации, которые находятся в процессоре маршрутизатора. Пример таблицы маршрутизатора M_1 для сети представлен в таблице 4.1.

Таблица 4.1 – Пример таблицы маршрутизации M_1

№ сети	**Сетевой адрес порта следующего маршрутизатора**	**Сетевой адрес выходного порта**	**Расстояние**	**Время жизни, *T***
L_1	Подключена	$M_1(1)$	1	X
L_2	Подключена	$M_1(2)$	1	X
L_3	$M_2(1)$	$M_1(3)$	2	X
L_4	$M_2(1)$	$M_1(3)$	2	X
L_5	$M_3(1)$	$M_1(4)$	2	X
L_6	Подключена	$M_1(4)$	1	X
L_7	$M_3(1)$	$M_1(4)$	2	X
Default	$M_3(1)$	$M_1(4)$	—	X

В этой таблице приведены только основные столбцы. На практике их больше. Первый столбец содержит IP-адрес сети назначения, т. е. сети, которой адресован пакет. Эти адреса условно обозначены L_1–L_7, хотя на самом деле это 32-битовые численные адреса, которые будут рассмотрены ниже. Во второй столбец заносится сетевой адрес порта маршрутизатора, на который следует отправить пакет для данной сети назначения, а в третьем столбце — адрес выходного порта M_1. Кроме того,

в четвертом столбце приведено расстояние между M_1 и сетью назначения в хопах (пройденных маршрутизаторах). Это нужно для сравнения альтернативных маршрутов и выборе кратчайшего. В столбец «Время жизни» заносится из проходящего пакета число пройденных им хопов, и оно уменьшается на единицу.

Рассмотрим работу маршрутизатора.

Аппаратное и программное обеспечение маршрутизаторов в зависимости от назначения и конфигурации может содержать набор физических интерфейсов (Ethernet, E1, SDH и др.), как это показано на рисунке 4.4. Канальный уровень также может быть представлен разными протоколами: MAC+LLC для Ethernet, PPP, LAP — F, LAP — D и др. Сочетание интерфейсов и протоколов можно регулировать сменными платами в оборудовании.

Пакеты (кадры), поступающие на порты маршрутизатора, после обработки с помощью протоколов первого и второго уровней освобождаются от заголовков канального уровня, при этом MAC-адрес преобразуется в IP-адрес с помощью протокола ARP (Adress Resolution Protocol). Полученные данные в случае неповрежденного пакета передаются модулю сетевого уровня, который анализирует IP-заголовок. Сначала проверяется контрольная сумма, затем время жизни. В случае положительных результатов из заголовка берется номер сети назначения, и он последовательно сравнивается с номерами сетей в таблице. Если в таблице найден нужный номер, то пакет направляется на соответствующий порт. Если же номера сети в таблице нет, пакет направляется на порт, соответствующий записи «default» — по умолчанию. Через этот порт наш маршрутизатор соединяется с глобальной IP-сетью. Это сделано для того, чтобы сократить объем таблицы маршрутизации, в которую заносятся адреса ближайших соседей. В IP-сетях в отличие от сетей на коммутаторах Ethernet существует несколько различных путей между узлами. Поэтому в таблицах маршрутизации для одной и той же сети назначения может быть несколько записей. Маршрутизатор при составлении маршрута выбирает оптимальный путь. Алгоритм процесса маршрутизации приведен на рисунке 4.5.

В заключение этого раздела следует сказать, что все аспекты деятельности IP-сетей описаны в документах RFC — Request for Comments. Эти документы можно найти на сайте http://www.ietf.org/rfc.html. Всего этих документов порядка трех с лишним тысяч. Их перечень дан в RFC 1543. Главными документами являются RFC 1112, 1123, 1812. Более подробную информацию об RFC можно найти в [10].

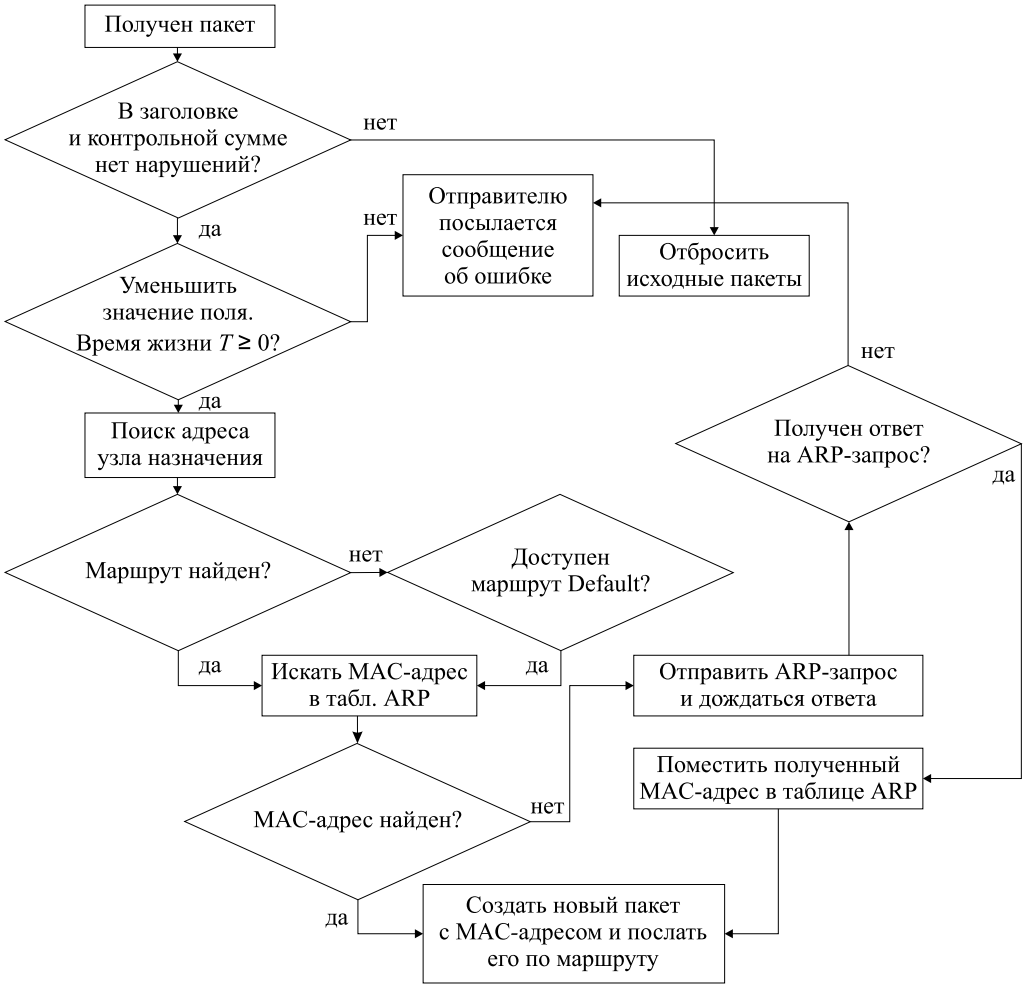
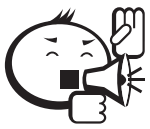


Рис. 4.5 – Алгоритм процесса маршрутизации

4.2 Адресация в IP-сетях

Для IP-адреса первоначально выбрали размер в 32 бита для удобства его обработки в 32-разрядном регистре компьютера.



Как уже говорилось, для обеспечения свойства иерархичности адрес содержит две части: номер сети и номер узла (станции), рисунок 4.6. Число бит, отводимых для этих номеров, может быть переменным.

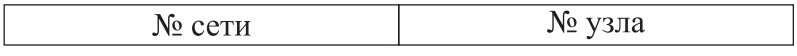


Рис. 4.6 – Структура IP-адреса

Пример IP-адреса — 192. 7. 65. 112. Здесь адрес приведен в десятичной системе исчисления. В двоичной системе этот же адрес будет: 11000000. 00000111. 01000001. 01110010. Для удобства идентификации байты адреса разделены точками.

Для того чтобы можно было присваивать адреса и малым, и большим сетям, ввели несколько классов адресов: *A*, *B*, *C* (рис. 4.7).

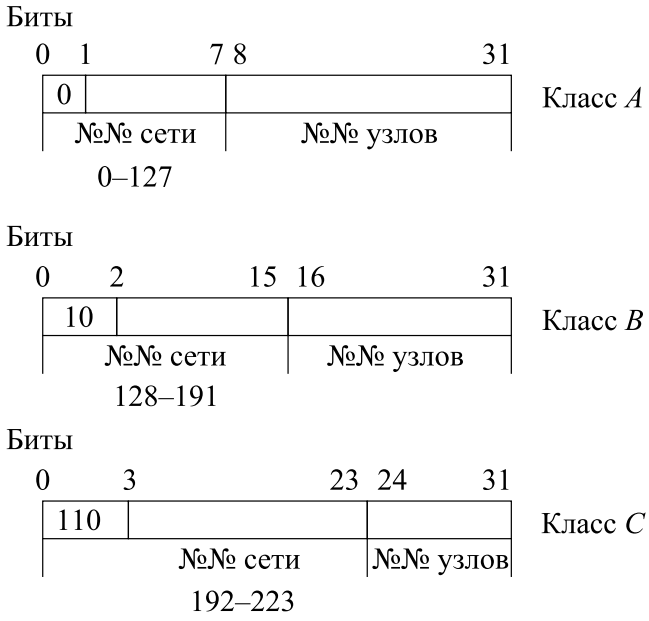


Рис. 4.7 – Адреса классов *A*, *B*, *C*

1. Адреса класса *A* предназначены для организации очень больших сетей. Они обязательно начинаются с 0. Всего таких сетей 128. В каждой из них может быть 16 777 216 (2^{24}) адресов станций (узлов), и их объем составляет 50% от общего количества всех IP-адресов.
2. Адреса класса *B* тоже дают возможность организовать достаточно большие сети в диапазоне номеров 128–191. Здесь под номер сети отводится уже два байта. Число сетей здесь — 2^{14} = 16 384, а максимальное число узлов в сети — 2^{16} = 65 536. Объем адресов класса *B* составляет 25%.
3. Адреса класса *C* содержат три байта для номера сети и один байт для номера узла. Следовательно, в одной сети класса *C* может быть не более 2^8 = 256 адресов, а таких сетей довольно много — 2^{21} = 2 097 152. Сети класса *C* — это небольшие сети. На самом деле максимальное число узлов сети меньше на два, т. е. 254 = 256 – 2. Это объясняется тем, что адреса, содержащие все единицы и все нули, являются специальными. Адрес 00000000 по умолчанию применяется, когда узел получателя находится в той же сети, что и адрес отправителя. Адрес 11111111 предназначен для широковещательной рассылки всем узлам данной сети (broadcast). Пример такого адреса 194. 67. 17. 255. Эти правила касаются и адресов типа *A* и *B*.

Кроме классов *A*, *B*, *C*, существуют специальные классы *D* и *E*. Адреса класса *D* (224 –239) используются для многоадресных рассылок в IP-сетях, когда одно сообщение распространяется среди группы разбросанных по сети станций. Адреса

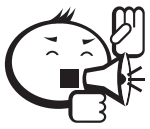
класса *E* (240 –255) составляют резерв, который может использоваться в экспериментальных целях.

Приведенное распределение IP-адресов является неэффективным при массовом распространении IP-услуг, так как системы распределения адресов оказались негибкими:

1. Сети класса *A* чрезмерно большие, и организации, их получившие, не в состоянии их распределить полностью. В то же время эти сети занимают половину адресного пространства.
2. Сети класса *C* лучше всего подходят для небольших организаций, но при этом резко возрастает количество самих сетей, что ведет к переполнению таблиц маршрутизаторов.
3. Сети класса *B* лучше всего подходят для построения больших сетей и дальнейшего распределения адресов. Но ресурс их адресного пространства быстро исчерпывается вследствие его ограниченности (25%) и бесконтрольного распределения на начальном этапе развития Интернета. Дело в том, что блоки по 65 тысяч адресов брали организации, которым требовалось гораздо меньшее их количество. Остальные адреса не использовались.

4.3 Подсети и маски

Для устранения названных недостатков были введены понятия подсетей и масок.



Суть нововведения заключается в том, что граница между номером сети и номером узла делается плавающей (рис. 4.8).

При этом может быть введен дополнительный номер подсети, который создает еще одно звено в иерархической адресной структуре — подсеть. Это позволяет разбить большие блоки адресов (прежде всего для классов *A* и *B*) на группы — подсети, размер которых уже может быть любым. Организация номера подсети осуществляется за счет адресного поля узла, т. е. из номера узла отводятся несколько бит для создания номера подсети. Так, для сетей класса *A* (рис. 4.8, *б*) число бит номера сети остается неизменным — 8, а число бит номера подсети может быть до 22. Минимальное число бит для номера узла — 2. Аналогично распределяются биты для сетей класса *B* (рис. 4.8, *в*) и класса *C* (рис. 4.8, *г*).

Рассмотрим, как нумеруются сети и подсети. В качестве примера возьмем сеть класса *B*. Здесь под номер сети отводится 16 старших бит 129.42.xxx.xxx. Индексами «x» обозначены позиции для подсети и узла. Чтобы номер сети отличить от номера подсети и узла, в адресных частях подсети и узла ставят нули — 129.42.0.0. Это сочетание цифр обозначает сеть класса B. Следует заметить, что 129.42.0.0 не является адресом сети, т. к. адрес имеют порты маршрутизатора, а сеть адреса иметь не может.

Аналогично обозначаются подсети. Так, для сети 129.42.0.0 подсети с числом станций до 254 будут идентифицированы как 129.42.2.0, 129.42.3.0 и т. д. Нетрудно

увидеть, что в этом примере сеть класса *B* расщепляется на несколько подсетей, каждая из которых эквивалентна сети класса *C*.

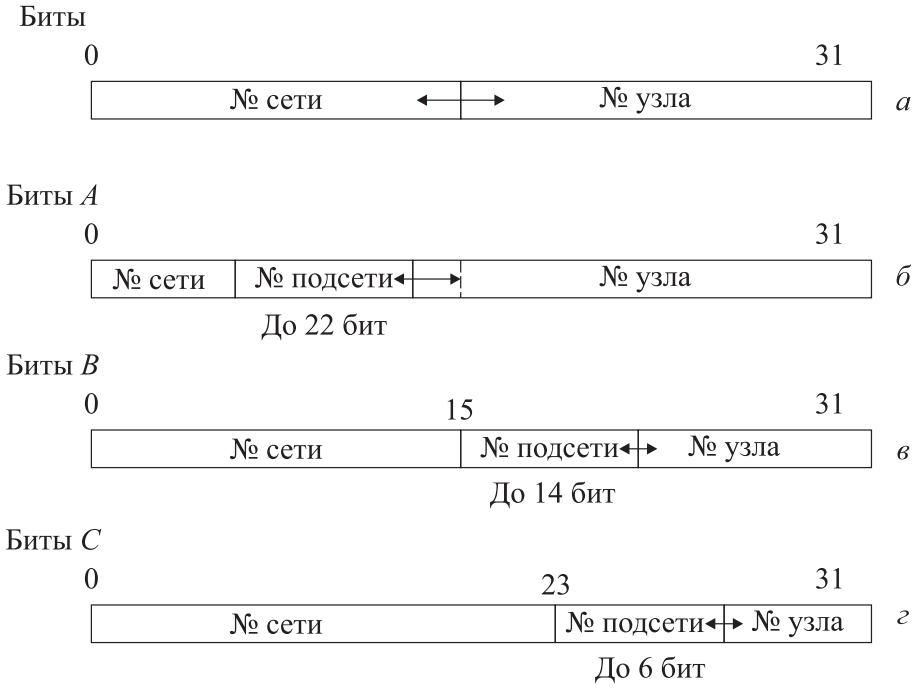
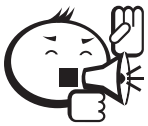


Рис. 4.8 – Введение подсетей

Несколько сложнее осуществляется нумерация подсетей, число станций в которых не совпадает с классом *C*. Для задания границы между подсетью и узлом вводится понятие маски.



Маска — это число, двоичная запись которого содержит единицы в разрядах, соответствующих номерам сети и подсети. Все единицы должны идти подряд, без пропусков. Маска используется совместно с IP-адресом.

Маску можно применить и для задания сетей. Так, для сетей класса *B* маска будет 11111111.11111111.0.0 или 255.255.0.0. Если нам нужно для сети класса *B* организовать, например, 5 одинаковых подсетей, то мы должны создать маску 11111111.11111111.11100000.00000000 (или 255.255.224.0). Три единицы в третьем байте дают возможность организации 8 подсетей ($2^3 = 8$). На самом деле это число должно быть сокращено до 6. Дело в том, что адреса станций, у которых в адресном поле одни нули или одни единицы, не используются (запрещенные комбинации).

Комбинации с непрерывной последовательностью нулей используются для идентификации сетей и подсетей. В рассмотренных ранее примерах будут использоваться следующие записи номеров сетей и подсетей:

129.42.0.0. → 01111011.00101010.00000000.00000000

129.42.3.0. → 01111011.00101010.00000011.00000000

Комбинации с непрерывной последовательностью единиц в адресном поле станции (т. е. после окончания маски) используются для широковещательной рассылки всем станциям подсети. Так, запись 123.42.255.255 означает, что пакеты рассылаются сразу всем станциям большой сети 123.42.0.0, а запись 123.42.3.255 говорит о широковещательной рассылке всем станциям подсети 123.42.3.0.

Полная информация о подсетях в сети класса *B* дана в таблице 4.2.

Таблица 4.2 – Подсети в сети класса *B*

Биты подсети	Количество подсетей	Биты для хостов	Количество хостов	Маска подсети
0	0	16	65 534	255.255.0.0
1	—	15	—	Недопустимая комбинация
2	2	14	16 382	255.255.192.0
3	6	13	8190	255.255.224.0
4	14	12	4094	255.255.240.0
5	30	11	2046	255.255.248.0
6	62	10	1022	255.255.252.0
7	126	9	510	255.255.254.0
8	254	8	254	255.255.255.0
9	510	7	126	255.255.255.128
10	1022	6	62	255.255.255.192
11	2046	5	30	255.255.255.224
12	4096	4	14	255.255.255.240
13	8190	3	6	255.255.255.248
14	16 382	2	2	255.255.255.252
	—	1	—	Недопустимая комбинация

На следующем этапе рассмотрим случай, когда с помощью маски 255.255.224 для сети класса *B* 129.42.0.0 требуется организовать пять подсетей одинаковой длины. Процедура и результат распределения номеров приведены в таблице 4.3.

Таблица 4.3 – Распределение номеров подсетей

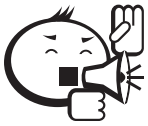
№ сети		№№ подсети	
десятичный	двоичный	двоичный	десятичный
Маска			
255.255	11111111.11111111	111|00000	224
129.42.0.0	01111011.00101010	000|00000	129.42.0.0 (запрещен)
⊣⊢	⊣⊢	001|00000	129.42.32.0
⊣⊢	⊣⊢	010|00000	129.42.64.0
⊣⊢	⊣⊢	011|00000	129.42.96.0
⊣⊢	⊣⊢	100|00000	129.42.128.0
⊣⊢	⊣⊢	101|00000	129.42.160.0
⊣⊢	⊣⊢	110|00000	129.42.192.0
⊣⊢	⊣⊢	111|00000	129.42.224.0 (запрещен)

Исходя из таблицы, число реальных подсетей будет 6, а их десятичные номера следуют не подряд, а через 32 единицы, поскольку под маской в третьем байте меняются биты в старших разрядах.

Ранее были рассмотрены подсети с масками постоянной или одинаковой длины. Однако их применение не является рациональным. Так, например, провайдеру Интернета нужно распределить IP-адреса сети класса *B* для разных пользователей, причем одному надо 6000 адресов, двум по 2 тысячи, а двум по 500 адресов. Раздавать всем адреса с помощью одинаковых масок 255.255.242.0 невыгодно. Поэтому надо для каждого класса пользователей применить свою маску. Так, для 6000 адресов потребуется 13 бит (2^{13} = 8192 > 6000 > 2^{12} = 4096). Следовательно, маска будет 11111111.11111111.11100000.00000000 или 255.255.224.0. Как видно, с такой маской адреса будут выданы с избытком (8190 – 6000 = 2190), который может быть использован для развития сети.

Для второго типа подсетей (2000 станций) найдем маску 255.255.248.0, а для третьего (500 станций) — 255.255.254.0.

Понятие маски вообще позволяет отказаться и от классовых адресов, и от понятия подсетей. Теперь достаточно передавать в заголовке IP-адрес и маску.



Поскольку передавать значения всех 32 бит маски нерационально, передают *префикс* — число, показывающее количество единиц в маске.

Например, для маски

11111111.	11111111.	11111110.	00000000
255.	255.	254.	0

префикс будет равен 23. В IP-адресе это выглядит так:

190.12.16.0/23

При использовании масок переменной длины возникает неопределенность в выборе маршрута, если подсети одной сети имеют разную длину. Суть этой неопределенности рассмотрим на примере (рис. 4.9).

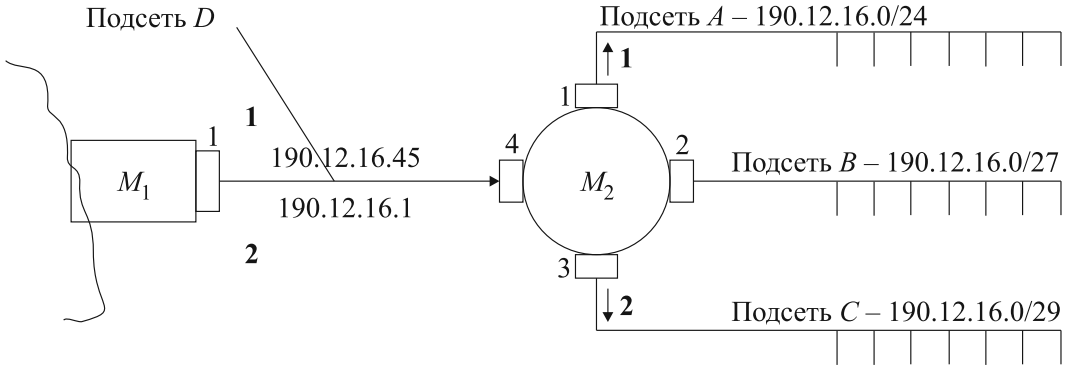


Рис. 4.9 – Распределение трафика в сети с масками переменной длины

Здесь сеть класса *C* 190.12.16.0 разделена на три подсети *A*, *B*, *C*. Самая маленькая из них — подсеть *C*. Она содержит всего 7 адресов 190.12.16.1–190.12.16.7. Подсеть *B* в соответствии со своей маской должна содержать 31 адрес (от 190.12.16.1 до 190.12.16.31). Но часть этих адресов уже занята в подсети *C*. Поэтому реально подсеть *B* содержит 24 адреса: 190.12.16.8–190.12.16.31. По этим же причинам подсеть *A* занимает не 255 адресов, а 223 (190.12.16.32–190.12.16.255).

Приведем сейчас таблицу маршрутизации для M_2 (табл. 4.4) и рассмотрим особенности распределения адресов и сам процесс маршрутизации.

Таблица 4.4 – Таблица маршрутизации M_2

Номер сети	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
190.12.16.0	255.255.255.0	192.12.16.32	192.12.16.32 (порт 1)	Подключено
190.12.16.0	255.255.255.224	192.12.16.8	192.12.16.8 (порт 2)	Подключено
190.12.16.0	255.255.255.248	192.12.16.1	192.12.16.1 (порт 3)	Подключено
190.12.17.0	255.255.255.248	192.12.17.3	192.12.17.3 (порт 4 M_2)	Подключено
0.0.0.0	0.0.0.0	192.12.17.4 (порт 1 M_1)	192.12.17.3 (порт 4 M_2)	—

В этой таблице три подсети (*A*, *B*, *C*) подключены к соответствующим портам маршрутизатора M_2. Каждый порт имеет IP-адрес из своей подсети, например порт 1 M_2 — 192.10.16.32. Для связи с внешним маршрутизатором M_1 необходимо организовать еще одну подсеть *D* и выделить для двух портов: 4 (M_2) и 1 (M_1) свои адреса. Пусть эта подсеть будет иметь номер 190.12.17.0. Так как сеть маленькая, для нее будет достаточно 8 адресов и маски 255.255.255.248.

Если на маршрутизатор M_2 поступает пакет с адресом 190.12.16.1–2, то маршрутизатор сравнивает его адресную часть со своей таблицей. Однако в таблице три почти одинаковые записи:

- 190.12.16.0/24;
- 190.12.16.0/27;
- 190.12.16.0/29.

В этом и заключается неопределенность. Чтобы ее разрешить, применяют правило максимальной длины: когда маршрутизатор обнаруживает сетевой адрес, которому соответствуют префиксы различной длины, он всегда выбирает маршрут с наибольшей маской. Поэтому пакет **2** будет направлен в подсеть *C*. Пакет **1** не будет принят этой подсетью, и его направят в подсеть *A*.

В таблице есть еще пятая строка с номером сети 0.0.0.0. Если на маршрутизатор M_2 поступают пакеты с IP-адресами, не принадлежащими подсетям *A*, *B*, *C*, *D*, то по умолчанию они будут направляться на внешний маршрутизатор M_1 и далее в глобальную сеть.

4.4 Распределение IP-адресов

Для распределения IP-адресов создана международная организация — «Комиссия по константам Интернет» (Internet Assigned Numbers Authority — IANA). IANA обладает абсолютными полномочиями и в своей структуре содержит три региональных отдела (рис. 4.10).

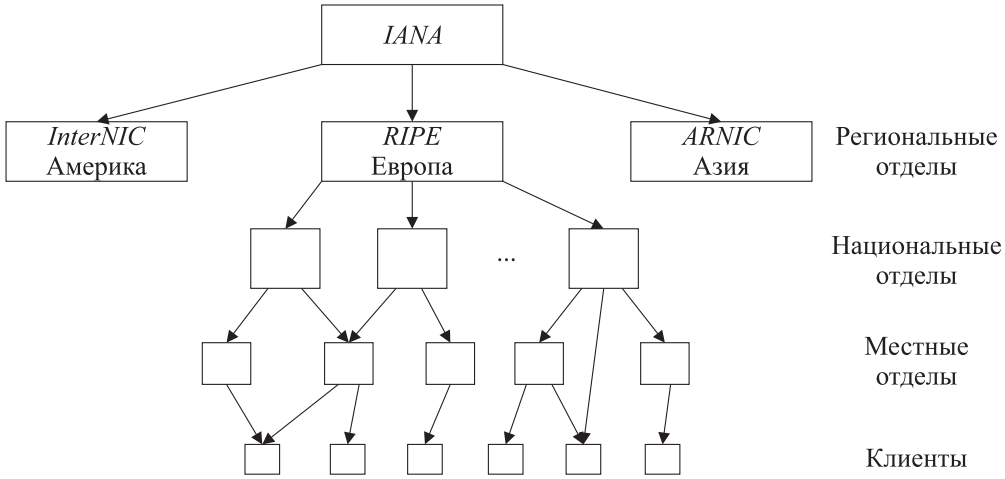


Рис. 4.10 – Структура распределения IP-адресов

Эти отделы распределяют адреса по различным государствам (национальные отделы), а те в свою очередь местным крупным провайдерам. Как правило, провайдеры получают блоки адресов сетей класса *C* или сети класса *B*. Далее провайдеры выдают адреса своим клиентам.

Как уже говорилось, при распределении IP-адресов наблюдается их дефицит и для преодоления этого используются *разные пути*.

1. Ранее рассмотренная технология подсетей и масок.

2. Использование в сетях предприятий и организаций собственных внутренних адресов, назначаемых произвольно местными администраторами. Эти сети соединяются с внешней сетью Интернет с помощью пограничных маршрутизаторов, которые имеют несколько стандартных IP-адресов. При получении пакетов маршрутизатор транслирует IP-адрес во внутренние адреса.

3. Применение динамических IP-адресов с помощью протокола Dynamic Host Configuration Protocol (DHCP). Эта процедура применяется широко при коммутируемом доступе к сети Интернет (рис. 4.11). Здесь значительное количество абонентов с помощью модемов (dial up, ADSL) подключаются к маршрутизатору *M* через модемный пул (множество модемов), расположенный на узле сети передачи данных.

Каждому модемному соединению DHCP-сервер выделяет произвольный IP-адрес из своего набора (пула) адресов. Разумеется, что в этом случае число используемых адресов значительно меньше числа абонентов.

Другим замечательным свойством DHCP является автоматизация выделения адресов по процедуре «клиент — сервер». Клиент (компьютер) посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер в ответ в своем сообщении направляет один из своих свободных IP-адресов на время сеанса

связи. После окончания сеанса IP-адрес изымается. Такая процедура назначения IP-адресов называется динамической. Она освобождает администратора сети от ручной малопривлекательной работы.

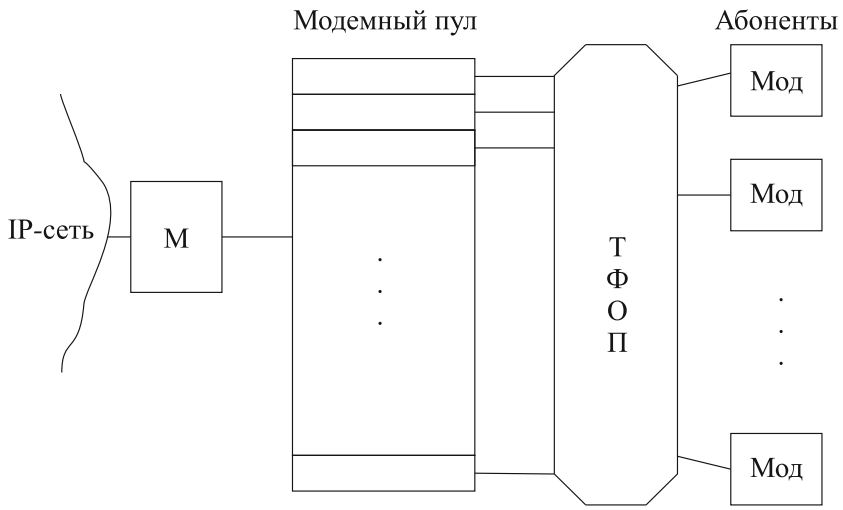


Рис. 4.11 – Коммутируемый доступ в IP-сеть

Кроме динамических IP-адресов есть статические адреса, которые выделяются абонентам в постоянное пользование. Назначение статических адресов может производиться либо вручную администратором, либо автоматически DHCP-сервером.

4. Наиболее радикальным способом является внедрение следующей версии IP-протокола — IPv6. Основные особенности следующие:

1) расширение поля адреса с 32 бит до 128 бит;
2) упрощение формата заголовка, удаление ненужных полей, постоянная длина 40 байт;
3) возможность маркирования потока;
4) возможность расширения заголовка;
5) возможность аутентификации и конфиденциальности.

4.5 Связь IP-адресов с другими системами адресации

Как было рассмотрено ранее, наряду с IP-адресами, рабочие станции, серверы, порты маршрутизаторов имеют еще и MAC-адреса (адреса сетевых карт), а также доменные (символьные) адреса. Все они используются одновременно, поэтому необходимы протоколы перехода от одной адресной системы к другой.

Рассмотрим вначале переход от доменных адресов к IP-адресам. Для этого создана специальная служба DNS (Domain Name System). Она содержит распределенную систему серверов (DNS-серверы), в которых размещаются таблицы соответствия «доменное имя» — IP-адрес для определенной группы символьных адресов, называемых доменом или поддоменом. Например,

— tomsknet.ru — 195.161.2.0

Процедура работы сервера следующая: абонент (рабочая станция) набирает доменное имя вызываемой стороны. Это может быть адрес сервера www, адрес электронной почты.

Станция обращается с запросом к DNS-серверу, обслуживающему поддомен, к которому относится абонент. Если сервер в своей таблице имеет информацию об IP-адресе вызываемой стороны, то он сразу дает содержательный ответ. Если же запрашиваемой информации нет, то сервер поддомена переправляет запрос на верхний уровень к корневому серверу DNS. Ответ по инстанции передается абоненту.

Переход от IP-адреса к MAC-адресу происходит при передаче IP-пакета на канальный уровень. Здесь также используются таблицы соответствия (табл. 4.5), которые устанавливаются протоколом ARP (Adress Resolution Protocol). Этим протоколом по IP-адресу находится MAC-адрес.

Таблица 4.5 – ARP-таблица

IP-адрес	MAC-адрес	Тип записи
193.112.76.40	004215DC7B21	Динамический
193.112.76.71	004215DC7B36	Статический
193.112.76.14	004215DC7B52	Статический

Считается, что станция-отправитель знает IP-адрес получателя. Если в ARP-таблице отправителя есть запись соответствия, то сразу происходит передача информации с использованием известных MAC-адреса и IP-адреса. Если же в ARP-таблице нет записи, то станция посылает в сеть специальный широковещательный ARP-запрос. Этот запрос посылается по IP-сети, так как IP-адрес получателя известен. Вместе с тем этот запрос помещается не в сам IP-пакет, а в пакет канального уровня. Так, в пакетах Ethernet есть специальное поле Type, содержащее 2 байта и определяющее тип передаваемого пакета (протокола верхнего уровня). Для протокола IP в поле Type используется код 0×0800, а для пакетов ARP код 0×0806. В качестве данных передаются MAC- и IP-адреса отправителя и получателя.

На ARP-запрос реагирует только та станция, которой он адресован. Получив запрос, она отправляет ARP-ответ, в котором содержится неизвестный MAC-адрес.

Все новые адреса станции по необходимости заносят в свои таблицы.

4.6 Протоколы маршрутизации в IP-сетях

Для того чтобы пакеты могли передаваться в IP-сетях, необходимы таблицы маршрутизации, которые находятся в маршрутизаторах. Эти таблицы могут составляться администраторами сетей вручную, но эти процедуры составления и обновления таблиц лучше выполнять автоматически. Для этого и служат специальные протоколы маршрутизации: RIP, OSPF, BGP и другие.

Эти протоколы не надо путать с сетевыми протоколами IP, IPX, X.25, которые были рассмотрены ранее.

При структуризации IP-сетей и распределении адресов вводится понятие автономной системы.

Автономная система (АС) — подключенный сегмент сетевой топологии, состоящий из набора подсетей и взаимодействующий через набор маршрутизаторов. Каждая автономная система имеет свой уникальный номер (сетевой адрес или префикс) и находится под единым управлением. Типичной автономной системой является сеть крупной компании или провайдера сетевых услуг. На рисунке 4.12 показана сложная сеть, состоящая из нескольких автономных систем. В составе этой сети есть магистральная сеть, которая представляет собой тоже автономную систему. Внутри каждой АС действует внутренний протокол маршрутизации IGP — Internal Gateway Protocol. В качестве IGP используются:

- RIP — Routing Information Protocol;
- OSPF — Open Shortest Path First.

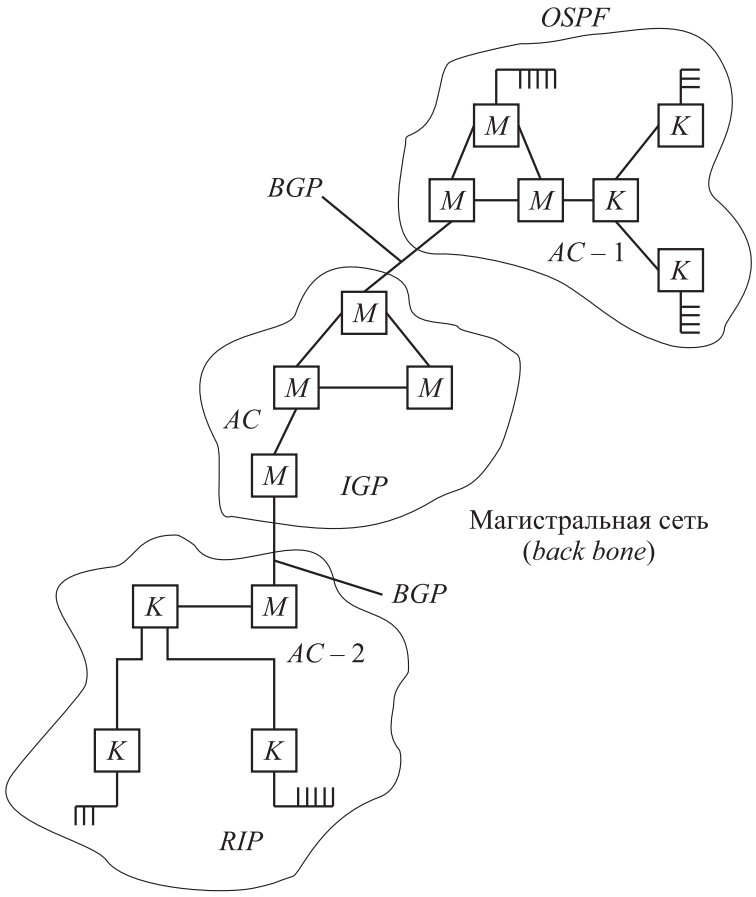


Рис. 4.12 – Сложная IP-сеть

Между АС действуют внешние протоколы маршрутизации:

- EGP — External Gateway Protocol;
- BGP — Border Gateway Protocol.

Связь АС происходит через пограничные маршрутизаторы, называемые шлюзами. Основной смысл разделения IP-сетей на АС — создание модульной и иерархичной системы, простой в управлении и способной к развитию. Простота управления

достигается тем, что для глобальной IP-сети автономная система представлена всего одним адресом внешнего маршрутизатора, да и то не всем, а только его старшими разрядами. Так, префикс 176.18.0.0/16 задает на внешнем шлюзе АС без излишней детализации. Все остальные адреса 176.18.xxx.xxx. находятся внутри системы.

Наряду с АС вводятся понятия:

1) «соседи» — маршрутизаторы, удаленные друг от друга на одно попадание («хоп»);
2) метрики маршрутизации — количественные характеристики, определяющие процедуру передачи пакетов. Они служат для сравнения и выбора маршрута;
3) протоколы маршрутизации, определяют процедуру составления таблиц маршрутизации. Они делятся на два класса:
   - протоколы вектора расстояния (distance vector). В этих протоколах либо считается число хопов между начальным и конечным пунктами — RIP, либо применяется более сложная метрика (пропускная способность, задержка, надежность доставки, стоимость и т. д.) — IGP, EGP;
   - протоколы состояния связей (link station). Здесь путем опроса маршрутизаторов создается карта всей сети и исследуется путь между двумя любыми заданными узлами. При этом также применяются различные метрики. Наиболее распространенный протокол — OSPF.

Содержание таблиц маршрутизации:

- адрес сети, подсети или системы назначения;
- IP-адрес маршрутизатора следующего попадания;
- сетевой интерфейс для доступа к следующему маршрутизатору;
- маска для точки назначения;
- расстояние до точки назначения (в хопах);
- время жизни в секундах от последнего изменения маршрута.

Рассмотрим теперь в качестве примера один из первых протоколов RIP (RFC 1058). Этот протокол анализирует маршрут на основе вектора расстояния, когда каждому хопу присваивается вес (обычно 1). Для каждого пути все веса суммируются, а затем из всех путей выбирается маршрут с наименьшей метрикой.

Для участка цепи, приведенной на рисунке 4.13, наилучшим маршрутом от сети A к сети B будет маршрут $M_1 - M_2 - M_4$.

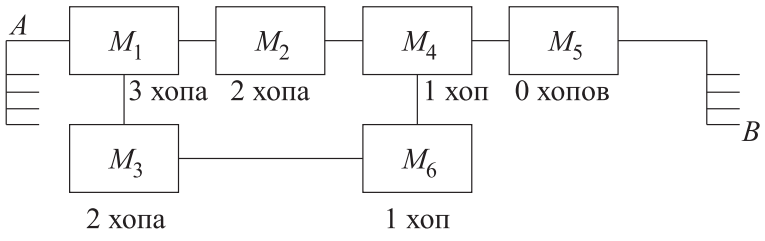


Рис. 4.13 – Выбор маршрута по протоколу RIP

Основные свойства протокола RIP:

1. Протокол очень простой. Он используется в небольших сетях.
2. Каждый маршрутизатор осуществляет широковещательную рассылку своих таблиц.
3. Имеется две версии: RIP v. 1 и RIP v. 2.
4. Протокол RIP v. 1 не поддерживает маски.
5. Все адреса различают только по классам *A*, *B*, *C* (для RIP v. 1).
6. В качестве метрики в RIP v. 1 используются только хопы.

Рассмотрим работу протокола RIP v. 1 на примере (рис. 4.14).

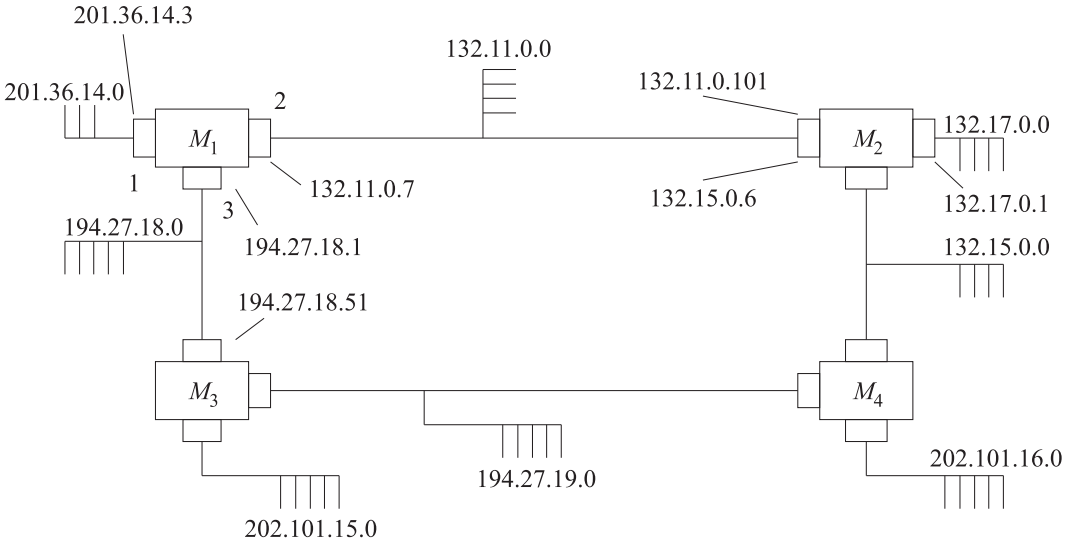


Рис. 4.14 – Пример IP-сети

Этап 1. Создание минимальных таблиц, фиксирующих начальное состояние (табл. 4.6). При этом учитываются только сети, непосредственно подключенные к маршрутизатору. Далее будем рассматривать маршрутизатор M_1. Для него минимальная таблица имеет вид.

Таблица 4.6 – Минимальная таблица начальных состояний для M_1

№ сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Аналогично составляются таблицы и для других маршрутизаторов.

Этап 2. Маршрутизаторы рассылают минимальные таблицы соседям. В нашем примере маршрутизатор M_1 отправит данные к M_2 и M_3.

Этап 3. Получение RIP сообщений от соседей, заполнение таблиц и обработка полученной информации. Таблица M_1 (табл. 4.7) на этом этапе будет выглядеть так.

Обработка здесь заключается в том, что если появляется повторная запись, то оставляется та, которая имеет наименьшую метрику. Если у двух записей метрики равны, остается та, которая появилась первой.

Таблица 4.7 – Таблица обработки информации

№ сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2

Этап 4. Рассылка новой таблицы соседям.

Этап 5. Получение RIP-сообщений и их обработка (повторение этапа 3).

В конечном итоге на всех маршрутизаторах устанавливается стационарное состояние, способное обеспечить передачу пакетов по протоколу IP.

Протокол RIP имеет ряд ограничений.

1. Время между рассылками составляет 30 секунд.
2. Максимальное число хопов, которое может пройти пакет, — 15. Если пакет использовал все хопы, он уничтожается.
3. Длина RIP-пакетов составляет 512 байт.

Простота протокола и эти ограничения приводят к появлению ряда проблем.

1. Если на появление новых маршрутов RIP-1 реагирует быстро, то к потере маршрутов он приспосабливается сложнее и медленнее, так как у него нет поля, которое сигнализирует о прекращении маршрута. Рассмотрим фрагмент сети, изображенный на рисунке 4.15.

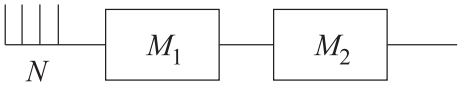


Рис. 4.15 – Фрагмент сети

Пусть сеть N стала недоступной. Маршрутизатор M_1 вносит в метрику значение 16 (недоступность объекта). Рассылку этой информации он начинает не сразу, а только тогда, когда наступает очередной 30-секундный интервал. Если до этого времени M_2 начнет свою рассылку, то M_1 увидит, что до сети N есть более короткий путь в 2 хопа (через M_2) и запись с метрикой 16 будет заменена. M_1 отправит в сеть информацию о том, что у него до N метрика равна 3. Таким образом, произойдет «зацикливание» и пакеты будут курсировать между M_1 и M_2 до тех пор, пока не закончится время жизни пакета. Исходя из вышесказанного можно сделать вывод, что RIP-1 хорошо работает в стационарных сетях.

2. RIP не может работать в больших сетях, так как максимальное расстояние между станциями — 15 хопов.

3. RIP работает с кратчайшими маршрутами, которые не обязательно самые быстрые (рис. 4.16).

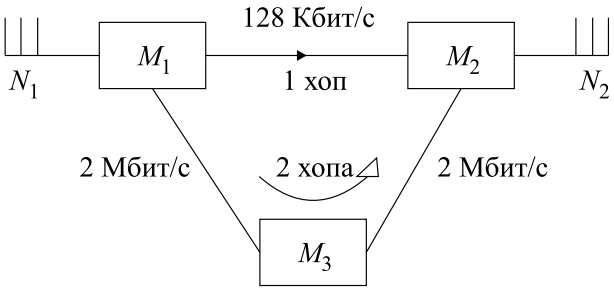


Рис. 4.16 – Неравноценность маршрутов по скорости

Протокол RIP-1 на рисунке изберет маршрут M_1 – M_3 – M_2. Этот недостаток возникает из-за того, что метрика единственная. Разницу в скорости можно компенсировать множителями: $1_{\text{хоп}} \times 2$, $1_{\text{хоп}} \times 3$ и т. д., но в этом случае сокращается диаметр сети.

4. Широковещательная рассылка RIP-пакетов перегружает сеть. Пусть, например, имеем 300 сетей. Для каждого IP-адреса выделяется 20 байт. Размер UDP-пакета 512 байт. Поэтому в одном UDP-пакете можно послать 25 адресов. Всего для 300 сетей потребуется 12 пакетов. Таким образом, каждый маршрутизатор через каждые 30 секунд посылает 12 широковещательных пакетов.

5. RIP-1 не работает с масками, как говорилось ранее.

Для устранения недостатков протокола RIP-1 применяют следующие меры:

- Метод расщепленного горизонта (split horizont).

Его суть заключается в том, что маршрутизатор не отсылает информацию о новом маршруте на тот порт, через который она была получена. Теперь в примере на рисунке 4.15 при обрыве сети *N* появится и останется метрика 16.

- Введение таймера неисправностей.

Получив информацию о недоступной сети, маршрутизатор игнорирует все последующие обновления о ней в течение 60 секунд.

Введение версии RIP v. 2, в которой предусмотрены авторизация (2 дополнительных байта), дополнительное поле для передачи наряду с адресом и маски и другие меры.

4.7 Виртуальные частные сети на базе стека протоколов TCP/IP

Виртуальные частные сети (VPN — Virtual Private Networks) организуют потоки данных одного предприятия, которые существуют в открытой сети с коммутацией пакетов и в достаточной степени защищены от влияния потоков данных других абонентов этой сети.

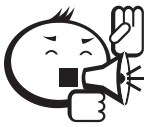
IP-адресация позволяет строить корпоративные сети любого масштаба и обладает рядом преимуществ:

- удаленный доступ к ресурсам ЛВС практически из любой точки, имеющей выход в сеть Интернет;
- высокая скорость передачи информации, ограниченная скоростью сети доступа;
- низкие затраты на создание сети, так как можно воспользоваться услугами провайдера Интернета (оператора связи);
- стоимость передачи IP-пакетов значительно меньше стоимости передачи трафика по цифровым каналом.

Основные недостатки VPN на базе IP-протоколов:

- сравнительно низкий уровень качества обслуживания (отсутствие гарантии заявленной пропускной способности и доставки пакетов);
- низкий уровень безопасности, который объясняется открытым характером сети.

Эти недостатки сейчас всячески нейтрализуются путем внедрения различных механизмов QoS и мер повышения безопасности (криптография, сетевые экраны и т. п.).



Таким образом, основное отличие VPN-IP от обычной IP-сети заключается в повышенном уровне безопасности, который может обеспечиваться практически на всех уровнях семиуровневой модели взаимодействия открытых систем.

В основе всех методов защиты лежит принцип инкапсуляции (туннелирования), рисунок 4.17. В этом случае IP-пакет снабжается аутентификационным заголовком, который включает в себя пакетный ключ и электронную цифровую подпись пакета (ЭЦП).

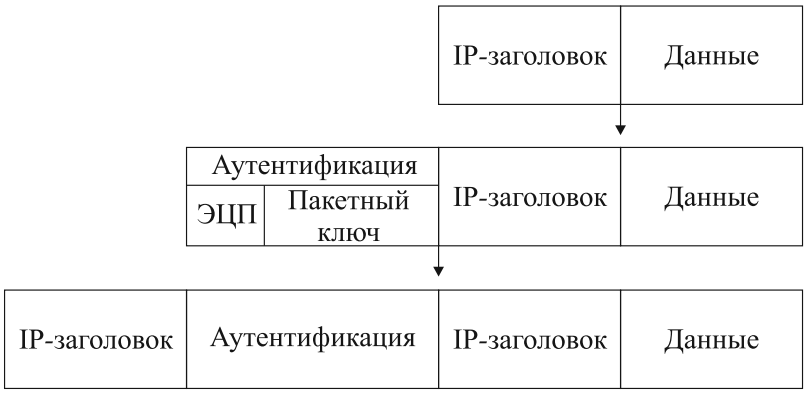


Рис. 4.17 – Инкапсуляция пакета VPN

Исходный пакет шифруется полностью вместе с заголовком. Этот зашифрованный пакет помещается в другой внешний пакет с открытым заголовком. Пакетный ключ также шифруется в пограничном устройстве (шифрующий маршрутизатор или межсетевой экран — МЭ). Для передачи данных по открытой сети использу-

ют открытые IP-адреса пограничных устройств. По прибытии внешнего пакета в конечную точку защищенного канала из него извлекают внутренний пакет, расшифровывают и используют его заголовок для дальнейшей передачи в частной сети.

Схема VPN приведена на рисунке 4.18.

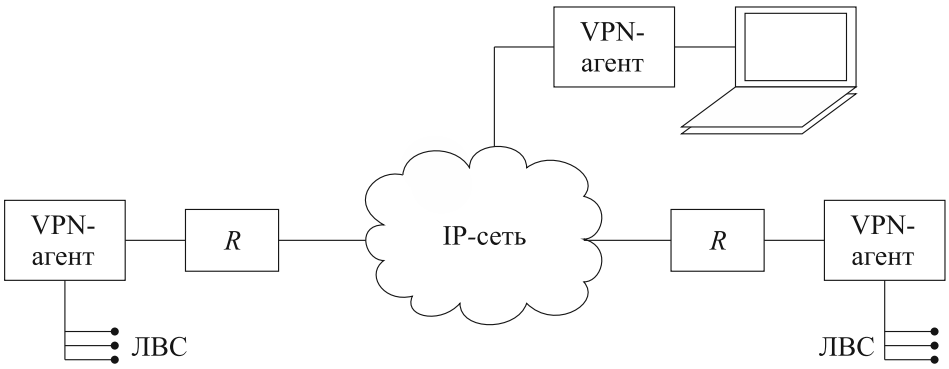


Рис. 4.18 – Схема VPN

Здесь VPN-агент может быть отделен от маршрутизатора *R*, а может быть совмещен с ним. В качестве протоколов в IP VPN сетях используют специальные протоколы. На канальном уровне — протокол PPTP (Point to Point Tunneling Protocol), который базируется на протоколе PPP в архитектуре клиент-сервер и использует механизм общей маршрутной инкапсуляции (GRE — Generic Routing Encapsulation) для передачи пакетов PPP. На сетевом уровне — протокол IPSec.

Он ориентирован только на протокол IP и решает следующие задачи:

- аутентификация пользователей;
- шифрование и аутентификация передаваемых данных;
- автоматическое снабжение конечных точек секретными ключами.

Кроме этих протоколов, существует множество других, работающих на всех уровнях семиуровневой модели ЭМВОС. Более подробные сведения можно получить в специальной литературе.

При реализации IP VPN следует учитывать следующие особенности. Дополнительные операции по защите каналов и данных приводят к увеличению доли служебной информации (перегрузка сети) и к увеличению задержки (падение производительности). Чем выше требования к конфиденциальности, тем сильнее проявляются эти факторы.

Вот некоторые данные, характеризующие падение производительности. Если процедура маршрутизации требует относительной вычислительной мощности — 1, то аутентификация пакетов — 12, а шифрование по алгоритму DES (Data Encryption Standard — Стандарт шифрования данных) — 22. Поэтому VPN, реализованные на базе маршрутизаторов, межсетевых экранов и персональных компьютеров, имеют производительность не более 10 Мбит/с. Для повышения производительности VPN применяют специальные процессоры.

Механизмы появления дополнительных задержек:

- установление защищенного соединения;

- шифрование и дешифрование данных;
- добавление нового заголовка к передаваемым пакетам.

Более всего на задержку влияет последний фактор. Так, например, в диспетчерских службах, в IP-телефонии размер передаваемых данных в пакете — 25 байт. Заголовки IP (24 байта) и PPP (~ 10 байт) увеличивают размер пакета до 60 байт. В то же время заголовок VPN SKIP содержит 112 байт, а заголовок IPSec — 54 байта. Таким образом, производительность падает в 2–3 раза.

Для надежной работы VPN также важно учитывать совместимость и поддержку стандартных протоколов VPN.

Варианты реализации VPN разнообразны:

1. Программные решения, когда программное обеспечение (обычно ОС Linux/Unix) устанавливается на обычном компьютере. Пример ОС FreeBSD — свободная UNIX-подобная операционная система.
2. Специализированное программно-аппаратное обеспечение. В этом случае применяются специально разработанные устройства в виде отдельных плат и специальное программное обеспечение, которые удаляют из пакетов все ненужные поля, чтобы ускорить процессы шифрования и передачи.

Известны следующие решения для VPN:

- VPN на базе операционных систем. Здесь сеть создается штатными средствами самой ОС. Наибольшее распространение получила система Windows NT/2000 и протоколы PPTP, PAP, GRE и IPSec. Это достаточно удобное и дешевое решение.
- VPN на базе маршрутизаторов. Здесь задача шифрования и дешифрования пакетов возлагается на них. Поддержка функции построения VPN включается во многие маршрутизирующие устройства.
- VPN на базе межсетевых экранов. МЭ — системы анализа трафика и блокировки доступа. На основе заданного набора правил МЭ анализируют пакеты на предмет разрешенных или запрещенных адресов и сервисов (TCP/UDP портов). Экран, как правило, состоит из двух механизмов: ограничительного и разрешительного. Система соответствующих фильтров разделяет сеть на несколько частей и обеспечивает избирательное прохождение пакетов между ними в соответствии с установленными классами защищенности.

Основные функции МЭ: администрирование, сбор статистики и предупреждение об атаке, аутентификация. Реализуются МЭ на базе маршрутизаторов, серверов уровня соединения (TCP) и прикладного уровня (telnet, ftp, proxy server и т. д.).

Контрольные вопросы по главе 4

1. Опишите суть передачи в IP-сетях в режиме «без установления соединения» (датаграммный метод).
2. Опишите режим передачи в IP-сетях «с установлением соединения» (метод виртуального соединения).
3. С какими протоколами канального и физического уровней работают IP-сети?
4. Как идентифицируются (нумеруются) IP-пакеты?
5. Назовите основные поля таблицы маршрутизации.
6. Какие преимущества при адресации дает применение масок?
7. В чем заключаются суть и целесообразность введения динамических IP-адресов?
8. Опишите процедуру перехода от DNS-адресов к IP-адресам а затем MAC-адресам.

Глава 5

СЕТИ ДОСТУПА

5.1 Понятие сетей доступа

В последнее время наряду с делением сетей связи на первичные, вторичные и т. д. чаще применяют другую классификацию, разделяя телекоммуникационные сети на транспортные или магистральные и сети доступа. Это связано с тем, что функции первичных и вторичных сетей начинают объединяться, поскольку цифровые сигналы, что от телефонии, что от терминалов передачи данных, имеют одинаковую структуру и между сетевыми узлами передаются цифровые потоки с мультисервисным содержанием. Поэтому под транспортной сетью понимают часть сети связи, включающую магистральные узлы, междугородные станции, а также те порты городских и районных станций, которые связаны с междугородными станциями. К транспортной сети относятся также каналы, соединяющие все вышеназванные станции.

Сеть доступа — это совокупность абонентских и соединительных линий, узлов концентрации нагрузки и станций местной сети, обеспечивающих выход абонентов через свои терминалы в транспортную сеть или местную сеть без использования транспортной сети. Поскольку сеть доступа является мультисервисной (телефон, данные, видео), то в ее составе необходимы узлы распределения по различным услугам. Обобщенная структурная схема сети доступа приведена на рисунке 5.1.

Здесь абонентские терминалы (АТ) — телефоны, модемы и т. п. — через сетевые окончания (СО) (розетки, разъемы) подключаются к сети доступа. От сетевых окончаний к концентраторам (К) или сразу к узлу распределения услуг (УРУ) идут абонентские линии (АЛ). Концентраторы, УРУ и узлы представления услуг (УПУ) связаны более скоростными соединительными линиями. Концентраторы нагрузки служат для уплотнения сигналов, идущих по абонентским линиям. Если сеть мультисервисная, то необходимы УРУ. Если услуга одна, то такой узел не нужен. В этом случае узел представления услуг будет один. Входные порты УПУ можно отнести к сети доступа, а выходные порты уже подключены к транспортной

сети. В последующих разделах мы подробней рассмотрим различные варианты сетей доступа.

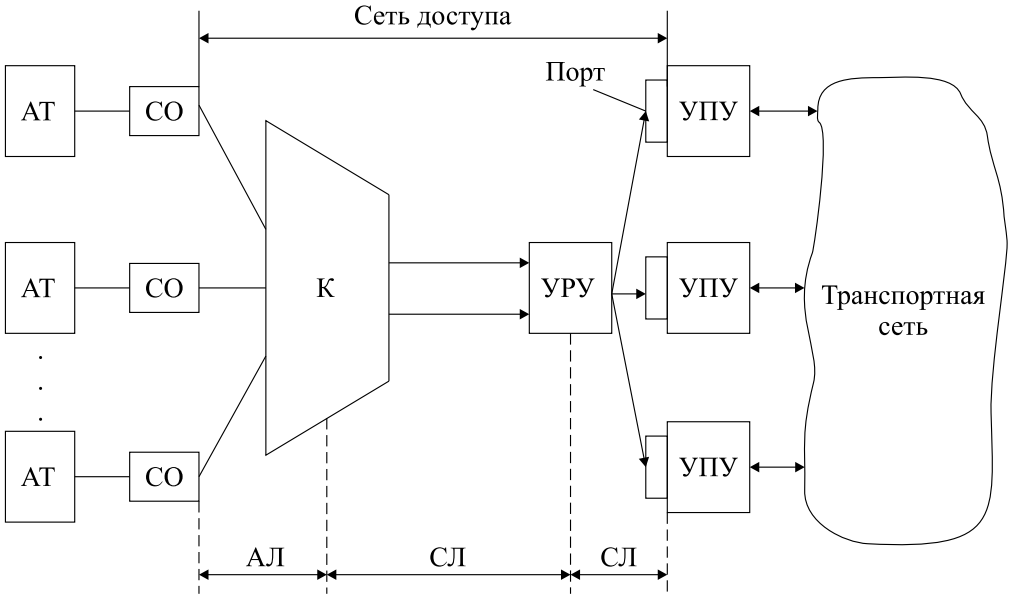


Рис. 5.1 – Структурная схема сети доступа

5.2 Доступ через телефонные сети

Телефонная сеть общего пользования представляет собой набор сетевых узлов и сетевых станций, связанных между собой системами передачи. К сетевым станциям подключаются сети доступа. В настоящее время доступ абонентов к телефонным сетям и сетям передачи данных осуществляется преимущественно по медным многопарным электрическим кабелям (рис. 5.2).

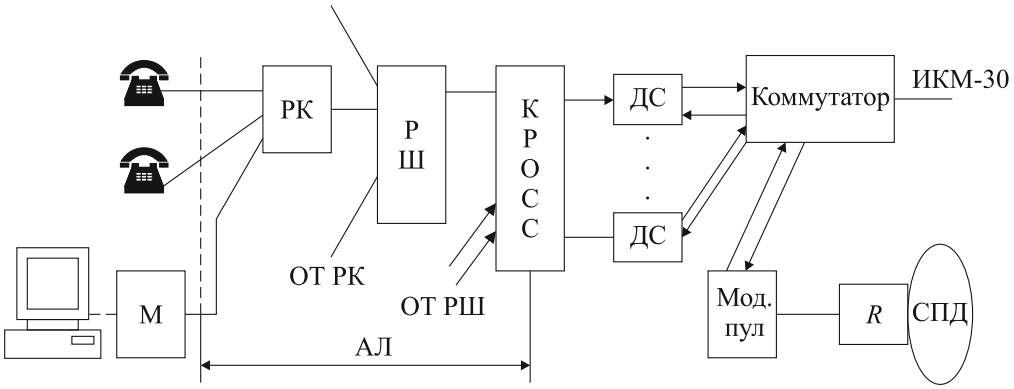


Рис. 5.2 – Сеть доступа на основе аналоговых абонентских линий

Здесь абонентские терминалы, аналоговые телефонные аппараты (формируют речевые сигналы в диапазоне 0.3–3.4 кГц) через телефонные розетки типа RJ-45 (сетевое окончание) подключаются к распределительным коробкам (РК) с помощью однопарных электрических кабелей типа ТРП. К выходу коробки подключен

уже многопарный кабель (обычно 10 пар). Кабели с РК поступают на распределительные шкафы (РШ), а затем на кросс, который располагается на АТС. Одна пара проводов, проходящая от абонента последовательно через РК, РШ и кросс, составляет абонентскую линию (АЛ). Далее с помощью дифференциальной системы (ДС) двухпроводное окончание преобразуется в четырехпроводное, с помощью которого абонентская линия подключается к порту коммутатора. В данном примере коммутатор является узлом предоставления услуг, поскольку вместе с системой сигнализации организует услугу телефонной связи. Ни концентратора, ни УРУ здесь пока нет, так как услуга одна.

Если через такую ТФОП с помощью модема *M*, модемного пула и маршрутизатора *R* организуется передача данных, то коммутатор уже начинает выполнять и роль УРУ, так как по серийному номеру модемного пула отделяет сигналы сети передачи данных (СПД) от телефонных. Для СПД узлом предоставления услуг будет маршрутизатор.

В последнее время в сетях доступа применяются мини-АТС или PBX (Private Branch Exchange). Их назначение — коммутация трафика абонентов внутри одного учреждения и передача внешнего трафика в ТФОП (рис. 5.3). Здесь число входящих линий (от абонентов) больше, чем число выходящих (к АТС).

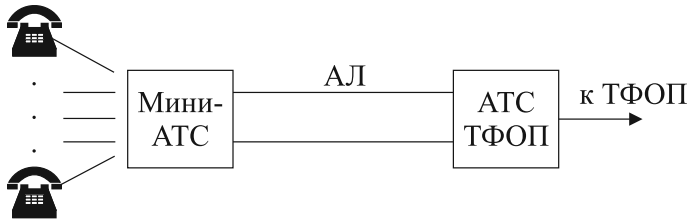


Рис. 5.3 – Включение мини-АТС в сеть доступа на аналоговых линиях

Поэтому абонентские линии, идущие к АТС, могут испытывать блокировку, но нагрузка в каждой линии (трафик) будет большой. Можно сказать, что мини-АТС выполняют также функции концентратора.

Мини-АТС наряду с аналоговыми портами могут иметь и цифровые, и порты Ethernet, и V.35 для подключения к СПД. Эти случаи будут рассмотрены ниже.

5.3 Цифровые сети доступа

Развитие транспортных цифровых сетей заставляет искать решения по цифровым сетям доступа с целью повышения качества и удобства телекоммуникационных услуг. Для этого цифровой сигнал нужно как можно больше приблизить к абоненту. В этом случае все или большинство компонент сети доступа должны функционировать с цифровыми сигналами. Рассмотрим возможные варианты.

5.3.1 Абонентские линии

Коммутируемые — на основе канала тональной частоты работают в полосе частот 0.3–3.4 кГц. Модемы с многоуровневой модуляцией, где число уровней квантования достигает 128, обеспечивают скорости передачи не выше 34 кБ/с (протокол

V.34) в двустороннем режиме и до 56 кБ/с (протокол K56Flex) при симметричном режиме передачи. Основной особенностью такого (аналогового) режима передачи является ограничение полосы пропускания и тот факт, что устройство АЦП и ЦАП находится на стороне АТС (рис. 5.4).

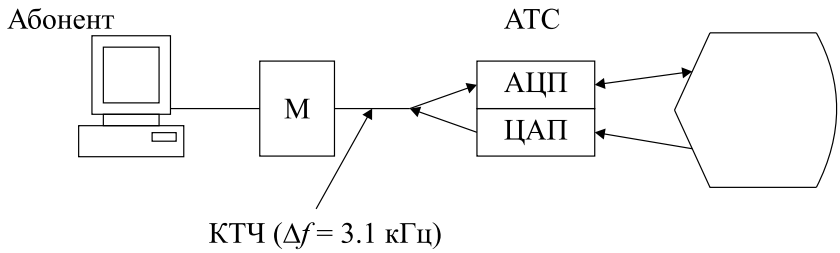


Рис. 5.4 – Модемное (dial up) соединение

В настоящее время этот метод доступа практически не применяется и здесь приведен с целью описания процессов развития технологий абонентского доступа.

5.3.2 Цифровые коммутируемые линии

В этих линиях цифровой сигнал формируется в терминальном оборудовании абонента (компьютер, цифровой телефон), а затем передается по линии связи но уже не в полосе 3.1 кГц, а в той, которую позволяет среда передачи. Средой передачи здесь является все та же пара или две пары медных проводов (рис. 5.5).

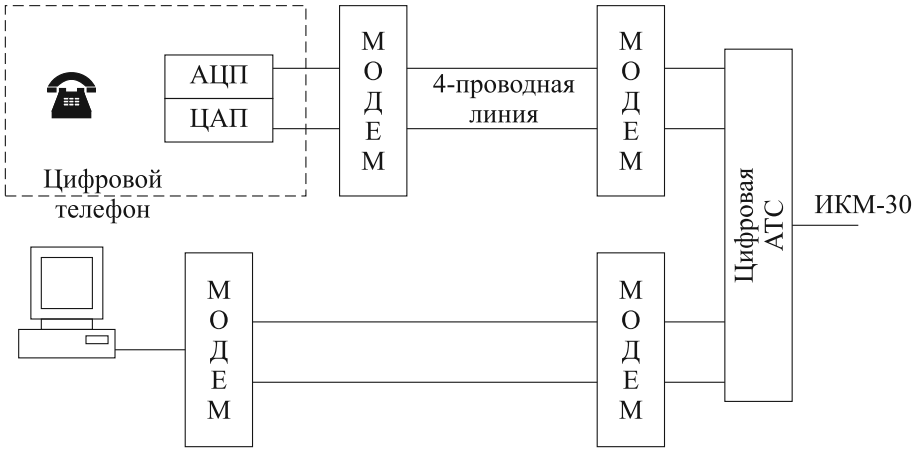


Рис. 5.5 – Цифровая линия доступа

Частотная характеристика затухания и волнового сопротивления двухпроводной линии на один километр длины приведена на рисунке 5.6.

Из него видно, что затухание увеличивается с ростом частоты, но эффективная полоса пропускания может быть значительно больше чем у КТЧ (3.1 кГц). Так, если допустить максимальную неравномерность затухания 75–80 дБ, то при полосе пропускания Δf = 500 кГц можно получить дальность действия линии в 3–5 км. Скорость передачи при этом можно увеличить за счет многоуровневого кодирования. Так, в соответствии с теоремой Шеннона пропускная способность канала связи в битах в секунду

$$B = \Delta f \cdot \log_2 \left(1 + \frac{S}{N}\right),$$

где S/N — отношение сигнал-шум в децибелах.

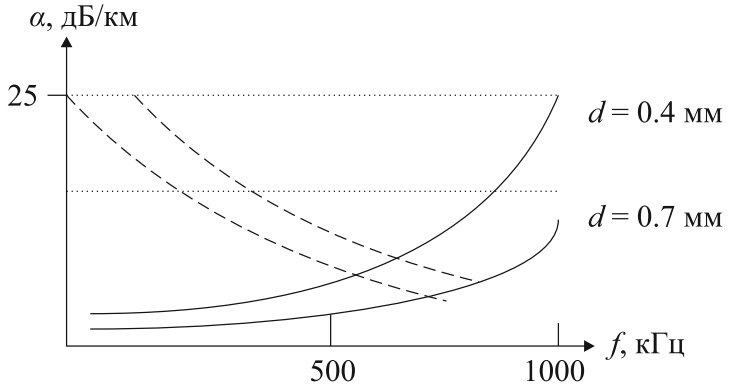


Рис. 5.6 – Частотная характеристика затухания в двухпроводной линии

При Δf = 500 кГц и шестнадцатиуровневом кодировании B = 2 Мбит/с.

Для реализации таких теоретических оценок разработано много разновидностей модемов для цифровых абонентских линий (ЦАЛ). Самым простым вариантом является использование линейного кодирования 2B1Q. Суть этого кода иллюстрируется рисунком 5.7, где изображены осциллограмма (*а*) и векторная диаграмма (*б*) цифрового сигнала. Здесь каждому временному интервалу соответствует одно из четырех состояний (4-уровневое кодирование).

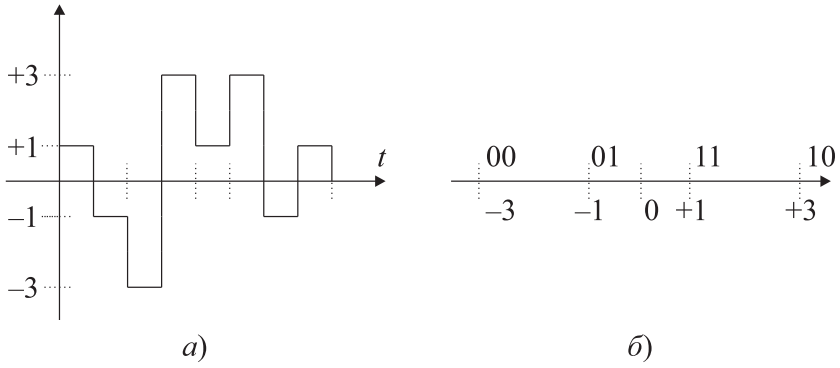


Рис. 5.7 – Диаграммы сигнала 2B1Q

Спектр сигнала 2B1Q изображен на рисунке 5.8. Из этого рисунка следует еще одно важное свойство таких модемов.

Поскольку сигнал биполярный, то его спектральные составляющие на низких частотах равны нулю. Следовательно, наряду с широкополосным сигналом в такой линии можно одновременно передавать сигналы КТЧ (телефонию).

Разумеется, что в модемах реализуется компенсация неравномерности частотной характеристики линии, эхокомпенсация и другие технические приемы для повышения качества и скорости передачи.

Вернемся теперь к коммутируемым цифровым абонентским линиям. В настоящее время на основании рекомендаций ITU-T разработан стандарт ISDN (Integrated

Services Digital Network) — цифровых сетей с интегральным обслуживанием. Этот стандарт предусматривает цифровой базовый доступ BRI по трем каналам $2B + D$, где B — канал со скоростью 64 Кбит/с, а D — цифровой канал со скоростью 16 Кбит/с.

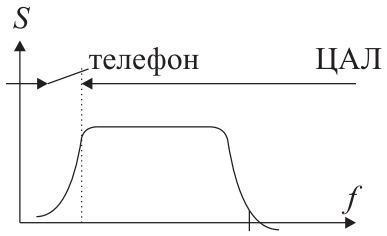


Рис. 5.8 – Спектр сигнала 2B1Q

Цифровой способ формирования и передачи в ISDN-BRI позволяет реализовать гибкую систему подключения абонентских терминалов. Так, возможны следующие режимы работы:

- одновременно работают два телефона,
- одновременно работает телефон и модем на скорости 64 Кбит/с,
- модем работает на скорости 144 Кбит/с.

5.3.3 Цифровые линии xDSL

Как уже говорилось в предыдущем разделе, по обычной медной линии можно передавать сигналы с шириной спектра до 1–2 МГц.

Применение многоуровневого или других видов кодирования позволяет получить скорости передачи данных до 50 Мбит/с.

Цифровые линии, использующие такие технологии — цифровые абонентские линии или, как сейчас чаще говорят, DSL — Digital Subscriber Line. Поскольку режим работы линии определяет модем, а разновидностей модемов DSL много, в литературе применяют такую аббревиатуру xDSL, где x и отражает индивидуальность модема и технологии.

В таблице 5.1 приведены типы модемов xDSL и их основные характеристики.

Как следует из таблицы, в зависимости от скорости передачи меняется и дальность действия модемов. Другой отличительной особенностью является необходимость использования двухпроводной или четырехпроводной линии для организации двусторонней передачи данных. Наконец, системы xDSL допускают передачу с одинаковой скоростью в обоих направлениях или асимметричный режим, когда скорость передачи информации к пользователю больше, чем от него.

Таблица 5.1 – Характеристики модемов xDSL

Тип	Название	Скорость, Мбит/с	Способ передачи	Число пар	Дальность, км
DSL	Digital subscriber line *(Цифровая абонентская линия)*	0.160	Дуплекс	1	8
HDSL	High — data rate DSL *(Высокоскоростная ЦАЛ)*	1.5 2.0	Дуплекс Дуплекс	2 2–3	3.5
ADSL	Asymmetric DSL *(Ассиметричная ЦАЛ)*	1.5–8 0.016–1	К абоненту От абонента	1	2.5–5.5
RADSL	Rate adaptive DSL *(Адаптивная по скорости ADSL)*	***Переменная*** До 8 До 1	К абоненту От абонента	1	2.5–5.5
VDSL	Very high data rate DSL *(Высокоскоростная ЦАЛ)*	13–52 1.5–2.3	К абоненту От абонента	1	0.3–1.5

Рассмотрим эти особенности подробней.

1. Поскольку полоса пропускания линии ограничена частотой 0.5 МГц, то получить высокую скорость передачи можно только за счет совершенствования модемов. К настоящему времени известны три основные технологии, применяемые при разработке модемов.

Кодирование 2B1Q. Этот метод используется в ISDN BRI и описан выше. Кроме того, он применяется в первых системах HDSL и MDSL. Разумеется, что эта технология более предпочтительна, чем ИКМ-30, так как позволяет передавать информацию со скоростью 2 Мб/с в полосе частот 500 КГц. Тем не менее затухание сигнала на высоких частотах и неравномерность волнового сопротивления очень велики, и это приводит к ухудшению качества передачи сигналов. К другим недостаткам кодов 2B1Q как следствие наличия высоких частот в спектре относятся:

- большой уровень перекрестных помех в соседних парах многопарного электрического кабеля;
- неравномерность АЧХ, ослабление высокочастотных спектральных составляющих, что уменьшает дальность действия модемов;
- искажение формы импульса и групповая задержка сигнала вследствие дисперсии фазовой скорости.

Таким образом, необходимы другие методы модуляции и кодирования, позволяющие уменьшить ширину спектра сигнала.

Технология CAP (Carrierless Amplitude and Phase Modulation). Эта технология позволяет существенно уменьшить влияние перечисленных недостатков технологии 2B1Q. Уменьшение ширины спектра сигнала здесь происходит за счет применения многоуровневой амплитудно-фазовой модуляции в сочетании с выделением одной (верхней) полосы частот модулированного сигнала. Несущая частота сигнала модулируется по амплитуде и фазе, причем число значений вектора сигнала составляет 64 и 128 (рис. 5.9).

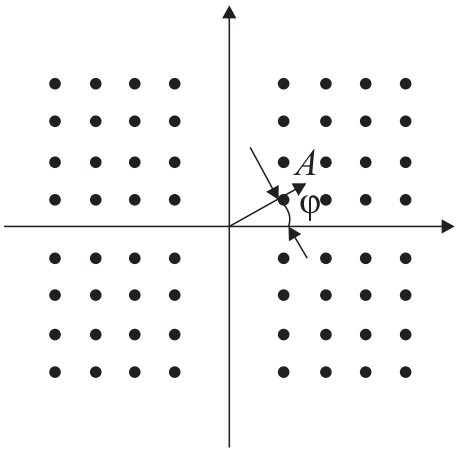


Рис. 5.9 – Диаграмма состояний CAP-64 сигнала: φ — фаза, A — амплитуда

Количество бит, передаваемых за одну посылку (бод), равняется

$$I = \lg l,$$

где l — число разрешенных состояний. При l = 64, I = 6, а при l = 128, I = 7. Таким образом, при CAP-64 за каждую посылку передается 6 бит информации, в то время как при 2B1Q их передается 2. Увеличение информационной скорости позволяет сократить тактовую частоту и существенно снизить полосу пропускания. На рисунке 5.10 приведены спектры сигналов 2B1Q и CAP-64 при одинаковой скорости передачи 1168 Кбит/с.

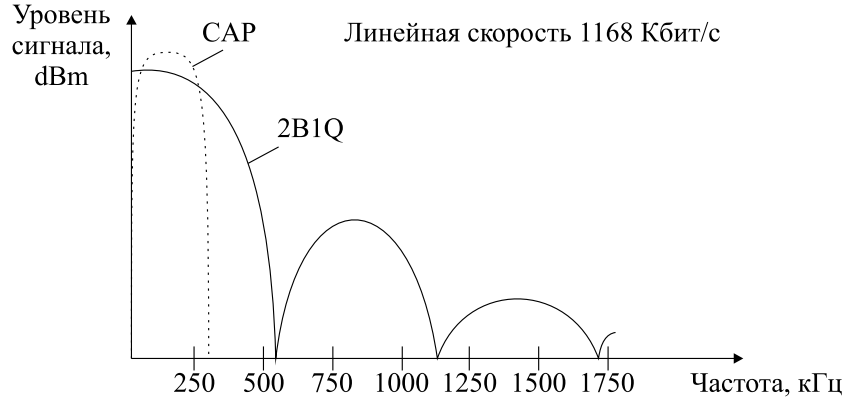


Рис. 5.10 – Сравнение спектров сигналов 2B1Q и CAP-64

Кодирование TC-PAM (Trellis Coded Pulse Amplitude Modulation). Здесь число уровней амплитудной модуляции по сравнению с 2B1Q увеличено до 16 и при-

менен метод решетчатого кодирования по алгоритму Витерби для повышения качества передачи (предсказание ошибок). Суть метода заключается в нахождении свертки последовательности входных битов с такой же последовательностью, но переданной на несколько тактов раньше. Сформированная так кодовая комбинация на приемном конце сравнивается с набором проверочных комбинаций и при этом выбирается наиболее близкая к принимаемой. В условиях сильных наводок и помех надежность передачи существенно возрастает. Это свойство кодов TC-PAM оказалось более значимым при построении модемов, чем незначительное расширение спектра по сравнению с CAP-64 или CAP-128. По сравнению с технологией 2B1Q коды TC-PAM выигрывают и по ширине спектра (в 1.5–2 раза) и существенно в помехоустойчивости.

2. Режим двусторонней передачи в xDSL системах возможен как по двум парам проводов, так и по одной паре.

Наиболее простым способом является передача сигналов для каждого из двух направлений по своей паре (пространственное разделение каналов). Типичным представителем такой технологии является HDSL, где используется модуляция 2B1Q и по каждой паре передается цифровой поток со скоростью 2 Мбит/с.

Размещение пар может быть либо по однокабельной, либо по двухкабельной схеме. В первом случае провода обеих пар находятся в одном многопарном кабеле, и здесь возможны наводки как на ближний, так и на дальний конец. При двухкабельной схеме, когда провода разных направлений размещены в разных кабелях, эти наводки минимальны. Основным недостатком такого метода передачи является необходимость выделения двух пар проводов, что дорого для абонента и не всегда возможно.

В связи с этим большинство разрабатываемых технологий xDSL сейчас позволяют организовать двустороннюю передачу по одной паре. Проблема разделения направлений передачи и приема решается тремя способами: 1) использованием дифсистем и эхокомпенсации, 2) разделением по времени, 3) разделением по частоте. Первый способ был описан ранее. Разделение по времени чаще всего реализуется как переключение направлений передачи (полудуплекс или метод «пинг-понг»), когда передатчики и приемники абонента и станции включаются поочередно. При синхронной передаче скорость уменьшается в два раза по сравнению со случаем двух пар.

При разделении направлений по частоте требуется более чем двукратное расширение полосы, если учесть защитный частотный интервал между двумя частотными диапазонами. Кроме того, этот метод требует применения аналоговых высокоизбирательных частотных фильтров, что дорого, громоздко и нетехнологично.

Поэтому в настоящее время для двусторонней передачи используют чаще всего дифсистемы или временной метод.

3. Симметричный режим передачи в системах xDSL реализуется как для двух, так и для одной пары.

К этим технологиям относятся ISDN BRI, HDSL, SDSL. Пропускная способность этих систем постоянна (см. табл. 6.1), что не всегда эффективно. Поэтому разработаны адаптивные технологии, когда скорость может регулироваться либо вручную, либо автоматически. При этом изменяется и дальность действия модемов.

Области применения симметричных модемов в сетях доступа следующие:

- замена ИКМ — трактов в соединительных линиях при увеличении длины участка регенерации до 25 км;
- подключение учрежденческих АТС;
- подключение корпоративных абонентов к сетям передачи данных регионального масштаба с целью построения своих сетей;
- скоростной доступ в Интернет организаций и частных пользователей;
- оказание мультисервисных услуг (телефон и Интернет, видеоприложения и Интернет).

Асимметричные технологии и прежде всего ADSL в первую очередь предназначены для скоростного доступа в Интернет, когда трафик из сети к абоненту гораздо больше, чем обратный, который содержит только запросы. Для того чтобы эта технология стала массовой, необходимо было использовать существующие двухпроводные абонентские линии без всяких переделок и с сохранением существующей телефонной связи (аналоговой или цифровой). Таким образом, для технологий ADSL необходимо применение линейных кодов, в спектре которых отсутствуют низкочастотные спектральные составляющие (рис. 5.8). При этом телефонный сигнал, спектр которого находится в области низких частот, не создает помех сигналу передачи данных. Разделение этих сигналов у абонента и на узле сети реализуется с помощью частотных разветвителей (фильтров), называемых также сплиттерами (рис. 5.11).

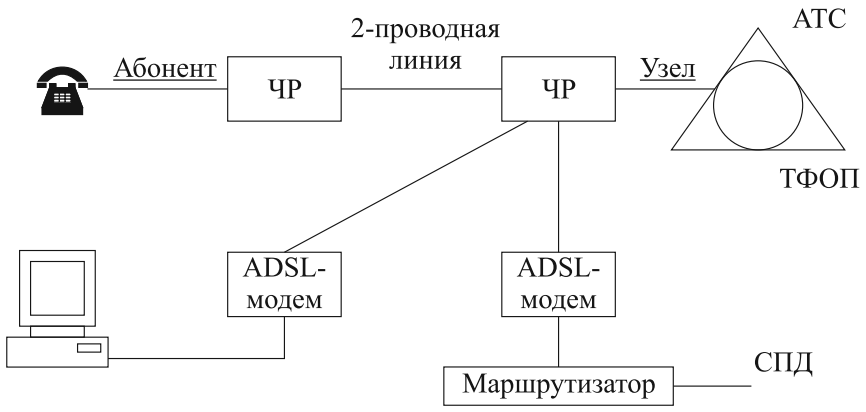
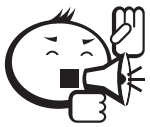


Рис. 5.11 – Схема ADSL-подключения



ADSL-технология является альтернативой режиму dial up.

Она наиболее эффективна на небольших расстояниях (до 3 км) при диаметре проводника электрической пары 0.4–0.5 мм. Обычно на узле модемы объединяются в стойку, называемую DSL Access Module (DSLAM). Как правило, DSLAM имеет порт Ethernet, к которому могут быть подключены коммутаторы, маршрути-

заторы и другие сетевые устройства. На участке между DSL модемом и DSLAM передаются три потока.

- Речевой телефонный (КТЧ) в диапазоне 0.3–3.4 кГц.
- Высокоскоростной цифровой поток к абоненту (downstream) со скоростями от 1.5 до 6 Мбит/с.
- Низкоскоростной цифровой поток от абонента (upstream) со скоростями от 15 до 640 Кбит/с.

Каждый цифровой канал может быть разбит на несколько низкоскоростных каналов, в которых скорость кратна величинам 1.536 Мбит/с или 2.048 Мбит/с. Эта процедура позволяет регулировать скорость, которая зависит от параметров телефонной линии (длина, диаметр провода, наличие дефектов и неоднородностей).

Для разделения перечисленных выше цифровых потоков применяют следующие методы. Как уже говорилось, сигнал КТЧ отделяется от цифрового сигнала сети передачи данных с помощью частотного фильтра. Разделение входящего и исходящего цифровых потоков реализуется двумя способами: 1) с частотным разделением каналов, 2) методом эхокомпенсации. В первом случае исходящий цифровой поток передается в полосе частот до 140 кГц, а входящий в полосе 0.14 –1.1 МГц. Для обеспечения высокой скорости передачи и ее регулирования применяется дискретная многотональная модуляция (DMT).

При эхокомпенсации применяют дифсистемы, встроенные в модемы.

Для дальнейшего совершенствования описанной технологии были разработаны ее модификации ADSL2 и ADSL2+. ADSL2 разработана в основном для увеличения скорости передачи на больших расстояниях в линиях с низкой помехоустойчивостью. Для этого в модемах применили более эффективную многоуровневую модуляцию и помехоустойчивое кодирование, сократили долю служебной информации. При этом удалось достигнуть прироста скорости на 100 кбит/с с одновременным увеличением дальности на 200 м.

ADSL2+, напротив, предназначена для работы на коротких линиях (< 1500 м). Расширение полосы пропускания двухпарного электрического кабеля до 2.2 МГц позволяет реализовать скорость передачи до 20 Мбит/с.

5.3.4 Системы передачи (соединительные линии)

Как уже говорилось ранее, соединительные линии идут от узла доступа к опорному узлу телекоммуникационной сети (АТС ТФОП, узел СПД и т. п.).

Как правило, по ним передаются цифровые потоки $n\times$E1 (ИКМ-30). Физической средой передачи могут быть:

- пары в многопарном электрическом кабеле в сочетании с xDSL модемами,
- волоконно-оптические линии связи (ВОЛС),
- цифровые радиорелейные линии (ЦРРЛ).

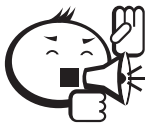
При построении сетей доступа на основе ВОЛС необходимо на узле доступа со стороны соединительной линии обеспечить преобразование электрического сигнала в оптический, и наоборот. Для этих целей применяют оптоволоконные модемы (оптические конверторы). В качестве передатчиков используются полупроводниковые лазеры с длиной волны λ = 0.85 мкм, 1.31 мкм, 1.55 мкм, а приемниками служат

быстродействующие pin-фотодиоды. Оптическое волокно может быть как одномодовое (SM), так и многомодовое (MM). Дальность действия таких соединительных линий: до 6 км (MM, λ = 0.85 мкм), до 100 км (SM, λ = 1.55 мкм). Интерфейсы доступа, кроме G.703–V.35, V.24, Ethernet. Скорости передачи до 1 Гбит/с.

Цифровые радиорелейные линии применяются в условиях малонаселенной и труднодоступной местности, в городских условиях, когда прокладка кабеля затруднена, а также в случаях, когда связь необходимо развернуть оперативно. Современные ЦРРЛ работают в частотных диапазонах от 400 МГц до 20 ГГц. Дальность действия определяется условиями прямой видимости (5–40 км 1 пролет). Скорость передачи — до 34 Мбит/с, интерфейсы доступа: G.703, V.35, Ethernet.

К недостаткам ЦРРЛ следует отнести: влияние осадков на качество передачи, необходимость высоких мачт для размещения антенн приемопередатчиков.

5.3.5 Узлы доступа



Как уже говорилось, абонентские линии объединяются в узлах концентрации нагрузки, роль которых могут выполнять узлы распределения услуг (УРУ) и узлы предоставления услуг.

Будем называть ту или иную совокупность этих устройств узлами доступа. Эти узлы бывают следующих типов:

- мультиплексоры,
- выносные концентраторы,
- учрежденческие или мини-АТС,
- коммутаторы сетей передачи данных,
- маршрутизаторы доступа.

Рассмотрим здесь мультиплексоры.

Абонентские мультиплексоры предназначены для объединения цифровых сигналов, поступающих от абонентов, и последующей передачи в одном скоростном цифровом потоке (рис. 5.12). Здесь происходит стандартное уплотнение во времени цифровых сигналов. Основное преимущество этой технологии — экономия количества пар в многопарном кабеле, а недостатки — неэффективное использование скоростного выходного канала и отсутствие внутренней коммутации. Сигналы абонентов, принадлежащих одному мультиплексору при их разговоре, будут передаваться на АТС и затем обратно к абонентам.

Число входных линий в абонентских мультиплексорах N может меняться от 2 до нескольких десятков и сотен. Типичным примером является мультиплексор ИКМ-30/32. В практике используются и мультиплексоры PCM-4, PCM-8 на 4 и 8 каналов соответственно, в которых используется кодирование 2B1Q и адаптивная дифференциальная импульсно-кодовая модуляция.

Гибкие мультиплексоры. Это мультиплексоры с большим набором функций и возможностей объединять и перераспределять различные входные сигналы. Так,

они могут выделить (вставить) из цифрового потока переменное количество каналов, могут осуществлять функции кросс-коннектора, т. е. программируемое переключение цифровых каналов как от одного входа к другому, так и к главным выходным потокам. Объединяемые (разделяемые) сигналы могут быть различными (цифровые потоки $n \times 64$ Кбит/с, E1 (2 Мбит/с), V.24/RS-232, ISDN BRI, xDSL, V.35, аналоговый телефон, Ethernet и др.). Физические интерфейсы тоже разнообразны (электрические двух- и четырехпроводные окончания, оптика, радиоканалы).

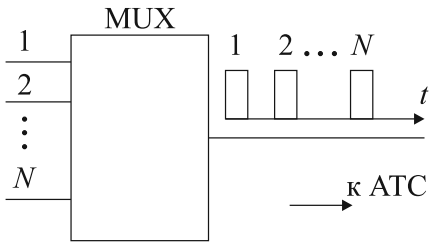


Рис. 5.12 – Абонентский мультиплексор (MUX)

Рассмотрим несколько примеров реализации гибких мультиплексоров.

1. Разделение цифрового потока на несколько компонентных потоков (рис. 5.13).

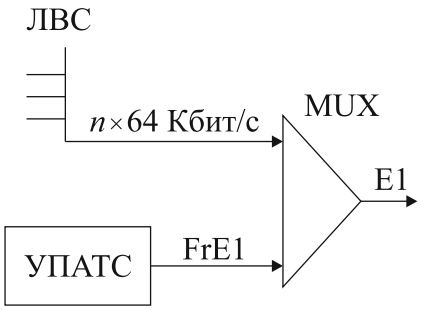


Рис. 5.13 – Мультиплексор доступа

Здесь поток E1 (2 Мб/с) разделяется на два. Один из них емкостью $n \times 64$ Кбит/с обеспечивает передачу данных от локальной вычислительной сети (ЛВС), а другой обслуживает учрежденческую АТС (УПАТС).

Гибкость мультиплексора заключается в том, что n может меняться от 1 до 31. В другом канале (Fractional E1) передаются оставшиеся цифровые каналы ($31 - n$).

2. Мультиплексор с интегрированием мультимедийного трафика (рис. 5.14).

Этот мультиплексор является более функциональным по сравнению с предыдущим. Здесь большое число входных портов, но что более важно, их назначение разнообразно. Здесь есть входы для обычных аналоговых телефонных линий, предусматривающих аналого-цифровое преобразование в цифровой сигнал со скоростью 32 Кбит/с и меньше. Есть входы для подключения компьютеров (V.24/RS-232), для скоростной передачи данных (до 2 Мбит/с) — V.35. Наконец, можно мультиплексировать потоки ISDN BRI или просто часть цифрового потока E1. По главной линии идет результирующий цифровой поток. Его скорость может быть различной — от 2 Мбит/с до $n \times 2$ Мб/с в зависимости от типа мультиплексора.

3. Мультиплексор с функциями кросс-коннектора (рис. 5.15).

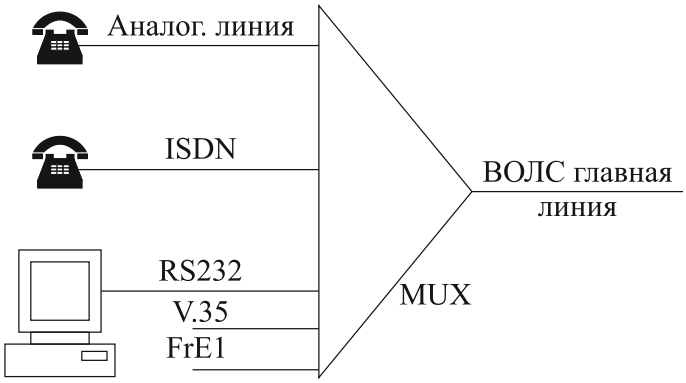


Рис. 5.14 – Мультиплексор для объединения разнородного трафика

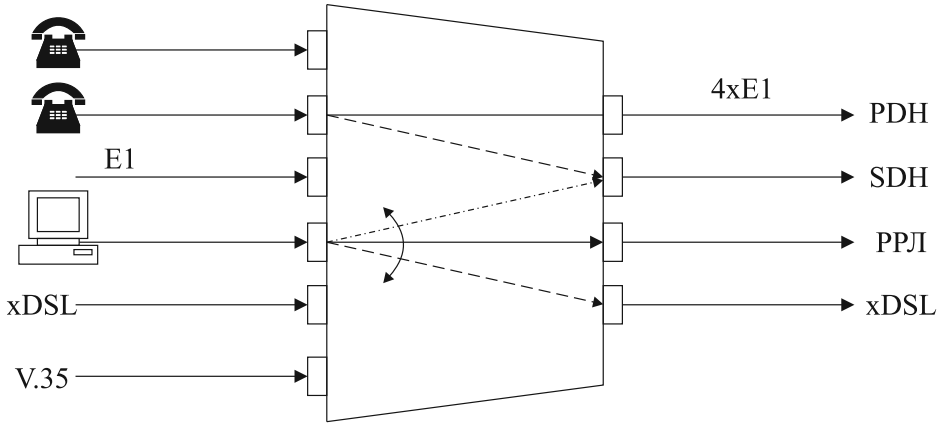


Рис. 5.15 – Интегральный узел доступа

Здесь, как и в предыдущем случае, на входе допустимы различные виды трафика, но мультиплексор (узел доступа) имеет четыре выхода. Трафик со входных портов может быть направлен на любой выходной порт. Эта процедура реализуется программным способом без блокировок и с созданием резервных маршрутов в случае неисправностей. Число входных каналов достаточно велико (например, узел Megaplex — 2200 фирмы RAD допускает 1200 каналов по 64 Кбит/с).

5.4 Доступ к сетям передачи данных

5.4.1 Общие сведения

В сетях передачи данных (СПД) роль АТС играет узел маршрутизации (маршрутизатор), к портам которого подходят соединительные линии от узлов доступа (узлов концентрации нагрузки). Узлов распределения услуг на сетевом уровне нет. Распределение услуг в стеке протоколов TCP/IP происходит на верхних уровнях.

Различные способы доступа к СПД представлены на рисунке 5.16.

Первый способ (dial up) осуществляется с помощью коммутируемых телефонных абонентских линий с помощью абонентских модемов M_1 и модемного пула (совокупность модемов), расположенного на узле доступа. Модемный пул содержит от нескольких десятков до нескольких сотен модемов, имеющих один серийный

телефонный номер. При наборе серийного номера абонентом его модем соединяется с любым свободным модемом на узле. Выход модемного пула подключен по цифровым каналам $n\times$E1 к порту маршрутизатора R. Скорость передачи и приема информации — десятки Кбит/с.

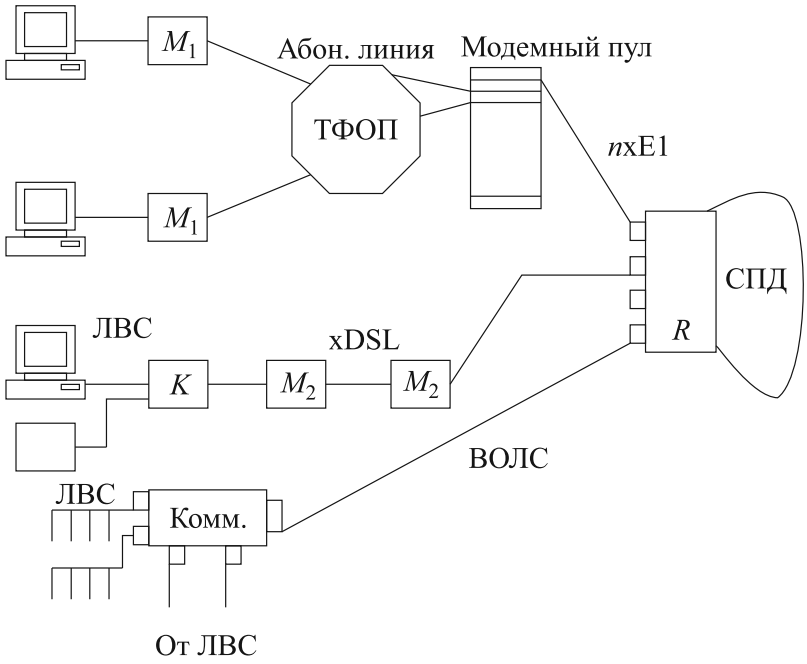


Рис. 5.16 – Организация доступа к сетям передачи данных

Второй способ реализуется для локальных вычислительных сетей (ЛВС) предприятий и организаций и отдельных абонентов. Здесь узлом доступа является концентратор (хаб) K, выход которого по скоростной линии xDSL подключен к маршрутизатору. Такой режим доступа абонентов (Ethernet) — является равноправным и случайным и поэтому сопровождается коллизиями (конфликтами). Вместе с тем он достаточно прост и дешев и широко применяется в компьютерных сетях. Скорость передачи данных может достигать от нескольких Мбит/с (Ethernet) до нескольких десятков Мбит/с (Fast Ethernet). Расстояние от станций (компьютеров) до концентратора до 100 м при использовании в качестве линии передачи витой пары и до 2000 м при использовании оптоволокна. Число портов концентратора невелико (до 72), но, включая их каскадно или по топологии «дерево», можно достичь значения 1024.

Третий способ аналогичен предыдущему. Он также предназначен для подключения к узлу СПД ЛВС, но в качестве узла доступа применяется коммутатор (switch). Основное достоинство этой схемы — отсутствие коллизий, поскольку коммутатор в отличие от хаба не транслирует пакеты с входного порта на все остальные, а создает соединение только с получателем по известному MAC-адресу. В качестве соединительной линии здесь могут применяться как ВОЛС, так и xDSL-линии и цифровые РРЛ. Длина линии от абонента до узла может достигать 2 км для многомодового оптоволокна.

Второй и третий способы работают на основе постоянного соединения (выделенная линия — on line) в отличие от первого, когда необходимо коммутируе-

мое соединение через ТФОП. Скорости передачи данных здесь существенно выше и могут достигать 100 Мбит/с (Fast Ethernet) и 1000 Мбит/с (Gigabit Ethernet).

В настоящее время широко применяются сети доступа на базе оптоволоконных технологий.

В них так применяются пассивные и активные схемы:

- пассивные на базе волоконных разветвителей, что эквивалентно технологии «общая шина»;
- активные на базе оптических коммутаторов.

5.4.2 Интерфейс V.35

В сетях доступа с использованием электрических кабелей на физическом уровне широко применяется интерфейс V.35. Этот протокол регламентирует постоянное модемное соединение в синхронном режиме передачи по выделенной линии. В качестве выделенной линии могут использоваться «прямые провода» (4-проводная линия) или аналоговая система передачи в многопарном электрическом кабеле или аналоговой радиорелейной линии с частотным разделением каналов. Для этих целей выделяются первичные (60–108 кГц) или вторичные (312–552 кГц) аналоговые широкополосные каналы.

Модемы используют синхронный дуплексный режим передачи по двум встречным каналам. Схема синхронного модема приведена на рисунке 5.17.

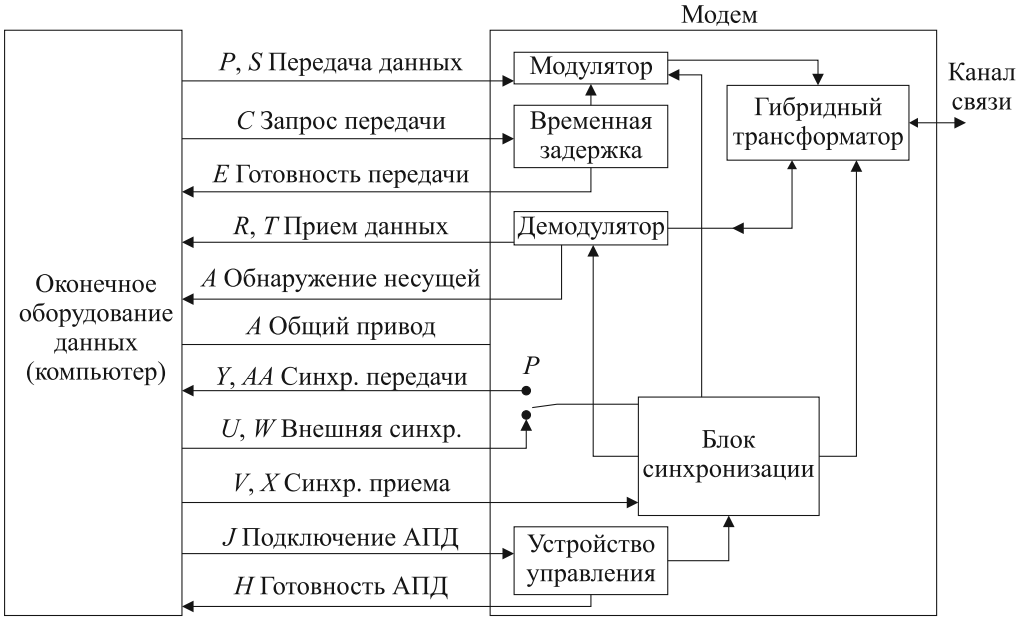


Рис. 5.17 – Схема подключения синхронного модема к оконечному оборудованию данных, где АПД — аппаратура передачи данных, *P* — переключатель

Здесь помимо функций «Обнаружение несущей», «Запрос передачи», «Прием и передача данных», характерных для асинхронных модемов, добавляются функции синхронизации приема, передачи и подключения модема.

В качестве физического интерфейса V.35 применяются либо разъемы M 34, либо разъемы DB-25 с 25 контактами. Высокочастотные сигналы (данные и синхросигналы) передаются по сбалансированным парам проводов, а управляющие сигналы (запросы, ответы, тесты и т. п.) — по одиночным проводам и общей шине.

Синхронные каналы передачи V.35 позволяют получить скорости передачи до 10 Мбит/с и используются в ГВС как в сетях доступа для подключения абонентов, так и для обеспечения связи с удаленными объектами, особенно в сельской местности.

5.4.3 Оптоволоконные сети доступа

Оптоволоконные сети доступа получили название FTTH (Fiber to the Home). В них оптоволокно доходит либо до дома (узел размещается в цокольном этаже FTTB (Fiber to the Building)), либо до квартиры.

В настоящее время в сетях доступа используются две технологии [9, 13]:

- технология пассивных оптических сетей (PON);
- технология на базе коммутаторов Gigabit Ethernet.

Широкое распространение получила архитектура Ethernet типа «звезда». Такая архитектура предполагает наличие выделенных оптоволоконных линий (обычно одномодовых, одноволоконных линий с передачей данных Ethernet по технологии 100BX или 1000BX) от каждого оконечного устройства к точке присутствия (point of presence, POP), где происходит их подключение к коммутатору. Оконечные устройства могут находиться в отдельных жилых домах, квартирах.

Другим вариантом FTTH является архитектура на базе PON (Passive optical network). При ее использовании для развертывания сетей FTTH оптоволоконная линия распределяется по абонентам с помощью пассивных оптических разветвителей с коэффициентом разветвления до 1:64 или даже 1:128. Нетрудно видеть, что эта архитектура представляет собой пассивное дерево, когда в точках ветвления нет активных элементов (коммутаторов).

Архитектура FTTH на базе PON обычно поддерживает протокол Ethernet (рис. 5.18).

В соответствии с рисунком входной поток данных (телефония, телевидение, компьютерные данные) от ONU разветвляется по многим направлениям и доходит до конечных пользователей. В терминальных устройствах ONT происходит разделение цифрового потока по трем видам услуг. Такой режим распределения информации является широковещательным, когда к каждому ONT подходит весь цифровой поток от ONU. Терминальные устройства должны выделить из него только свою частную информацию.

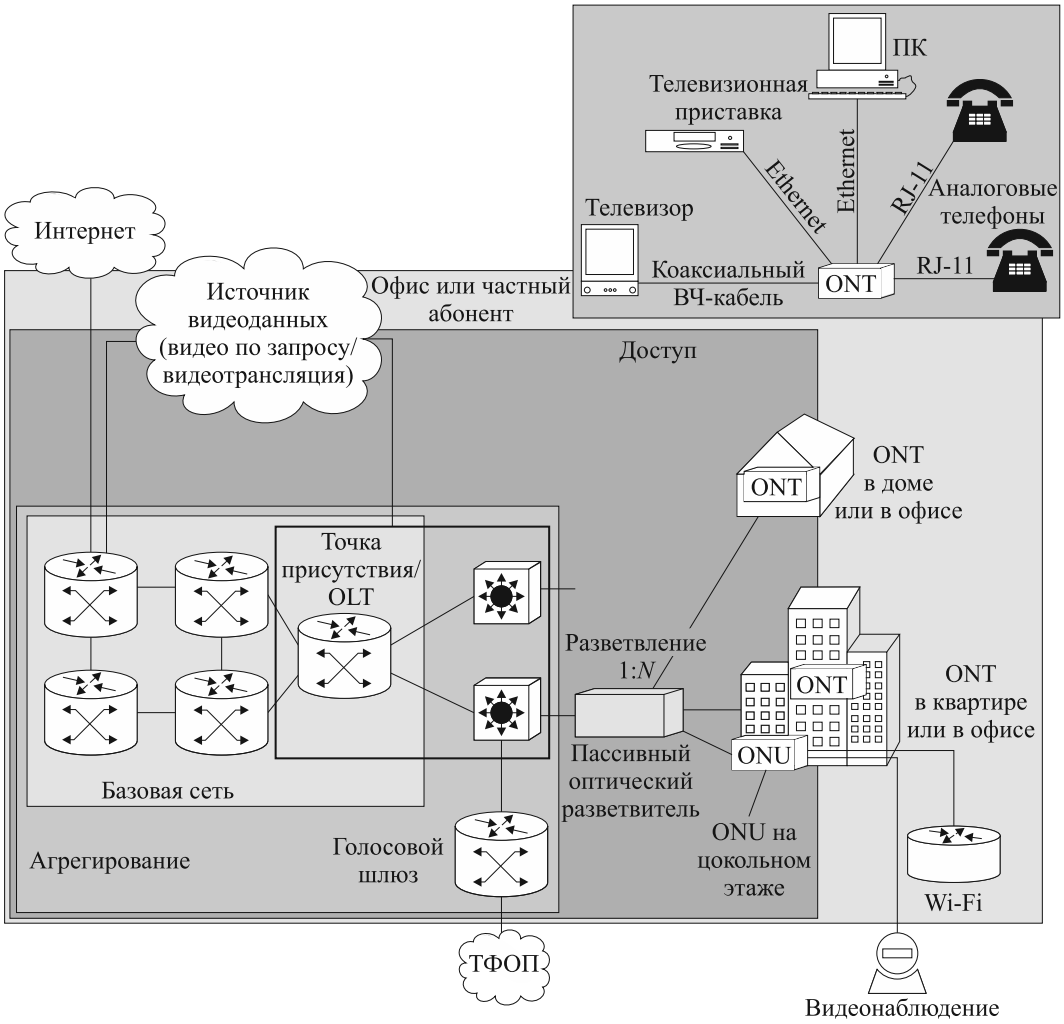
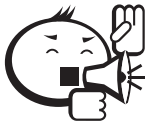


Рис. 5.18 – Архитектура пассивной оптической сети (PON)



Для обеспечения режима интерактивности в GPON используется та же пассивная волоконно-оптическая сеть, только восходящий трафик (телефония, IP-запросы) передаётся на другой длине волны.

В частности, для наиболее простых систем нисходящий трафик передается на длине волны 1490 нм, а восходящий на длине волны 1310 нм. В некоторых случаях используется дополнительная длина волны нисходящего потока (downstream), что позволяет предоставлять традиционные аналоговые и цифровые телевизионные услуги пользователям без применения телевизионных приставок с поддержкой IP.

Применяются следующие стандарты сети PON. Параметры полосы пропускания обозначают совокупную скорость передачи данных в нисходящем и восходящем потоках. Эта скорость передачи данных делится между 16, 32, 64 или 128 абонентами, в зависимости от плана развертывания. EPON была разработана с целью снижения стоимости путем использования технологии Gigabit Ethernet, архитектура GPON разрабатывалась, чтобы обеспечить более высокую скорость

передачи данных нисходящего потока, снизить накладные расходы и обеспечить возможность передачи трафика ATM и TDM. Архитектура GPON используется в качестве транспортной платформы Ethernet.

GPON (Gigabit PON) — перспективный стандарт PON ITU G.984 (2005). Транспортный протокол — GFP (generic framing protocol). Нисходящий поток — 1490 нм, 2.4 Гбит/с или 1.2 Гбит/с. Восходящий поток — 1310 нм, 1.2 Гбит/с или 622 Мбит/с. В 2008 году принят стандарт GPON ITU G.984.6 (2008), с поддержкой до 128 абонентов на дерево на расстоянии до 60 км.

Технология GPON способствует эволюции телевидения от широковещательного (multicast) до персонального (unicast, Video-on-Demand) с качеством HDTV практически для всех абонентов. Видеоканал в HDTV качестве занимает до 20 Мбит/с, то есть 1.2 Гбит/с для 64 абонентов в сегменте PON, что вдвое меньше ширины нисходящего канала в GPON (2.5 Гбит/с). GPON предоставляет масштабируемую структуру кадров при скоростях передачи от 622 Мбит/с до 2.5 Гбит/с, поддерживает как симметричную битовую скорость в дереве PON для нисходящего и восходящего потоков, так и ассиметричную и базируется на стандарте ITU-T G.704.1 GFP (generic framing protocol, общий протокол кадров), обеспечивая инкапсуляцию в синхронный транспортный протокол любого типа сервиса (в том числе TDM).

К другим преимуществом технологии PON следует отнести минимизацию активных устройств и портов. Они присутствуют только в ONU. Оптоволоконный кабель устойчив к электромагнитным воздействиям, не является источником электромагнитных волн, привлекателен по массогабаритным параметрам и защищен от несанкционированного доступа. Инфраструктура GPON отличается крайней неприхотливостью и безопасностью: не требует электропитания и может быть смонтирована в любом, даже неприспособленном помещении.

Проблемы PON-архитектуры

При развертывании архитектуры пассивной оптической сети PON возникают несколько проблем.

Общая полоса пропускания. Полоса пропускания в дереве оптоволоконных линий сети PON используется как можно большим числом абонентов, что позволяет получить прибыль за счет снижения затрат на каждого абонента. Хотя технология GPON обеспечивает общую пропускную способность нисходящего потока, равную 2.5 Гбит/с, она не может соответствовать росту сервисов и будущих требований абонентов в долгосрочной перспективе, поскольку потребности в пропускной способности растут экспоненциально. Более того, некоторую часть полосы пропускания необходимо резервировать для потоковых услуг (например, IPTV), что приводит к сокращению общей полосы пропускания.

Шифрование. Поскольку PON — это технология с общей средой передачи, то необходимо шифрование всех потоков данных. В технологии GPON проводится шифрование только нисходящего потока, а использование надежного усовершенствованного стандарта шифрования (Advance Encryption Standard, AES) с 256-разрядными ключами позволяет повысить безопасность личной информации конечных пользователей и предоставляет сервис-провайдерам возможность предотвратить хищение услуг. Однако надежность стандарта AES обусловливает снижение производительности. Для шифрования необходима передача существенного объема служебной информации вместе с каждым пакетом, что может привести к замет-

ному снижению полезной скорости передачи данных в PON (в зависимости от сочетания различных видов трафика).

Высокая рабочая скорость передачи данных. В связи с использованием в пассивных оптических сетях PON общей передающей среды, каждое оконечное устройство (ONT) вынуждено работать на совокупной скорости передачи данных. Даже если клиент заплатил только за 25 Мбит/с, каждая конечная точка оптической сети (ONT) в этом дереве PON должна работать на скорости 2.5 Гбит/с (GPON). Работа электронных и оптических устройств со скоростью, в 100 раз превышающей необходимую скорость передачи данных, повышает цену компонентов, особенно в том случае, если объемы производства не слишком большие.

Необходимость большей мощности оптического сигнала. При каждом разветвлении в соотношении 1:2 энергетический потенциал линии связи падает на 3.4 дБ. Следовательно, при разветвлении в соотношении 1:64 энергетический потенциал линии связи уменьшается на 20.4 дБ (эквивалентно отношению мощностей 110). Таким образом, в этой модели все оптические передатчики в архитектуре PON должны обеспечивать в 110 раз большую мощность оптического сигнала по сравнению с архитектурой FTTH «точка-точка» при передаче на то же расстояние.

Доступ абонента. Обычно при развертывании сети FTTH выполняется одновременное подключение оптоволоконных линий связи для всех потенциальных абонентов в данном районе. В случае пассивной оптической сети все эти оптоволоконные линии затем подключаются к разветвителям и стягиваются фидерным оптическим кабелем к центральной АТС или точке присутствия. Абоненты могут подписаться на сервис FTTH только после развертывания всех оптоволоконных линий. При развертывании услуг для частных абонентов сервис-провайдеры редко достигают 100-процентной подписки. Обычно этот показатель близок к 30 процентам, что означает, что структура PON сети используется не оптимально, а стоимость оборудования ONT для каждого абонента значительно возрастает. Одним из решений этой проблемы является использование удаленных оптических распределительных узлов. Однако применение этого оборудования предполагает дополнительные затраты, которые обычно не компенсируются улучшением загрузки пассивной оптической сети PON.

Обслуживание, поиск и устранение неисправностей. Пассивные оптические разветвители не могут передавать информацию о неисправностях в центр управления сетью. Поэтому с помощью обычного оптического временного рефлектометра (OTDR) очень сложно обнаружить какую-либо неисправность оптоволоконной линии между разветвителем и точкой терминации оптической сети (ONT) абонента. Это значительно усложняет поиск и устранение неисправностей в сетях PON и повышает затраты на их эксплуатацию.

Устойчивость. При повреждении точки терминации оптической сети (ONT) она может передавать в дерево оптоволоконных линий постоянный световой сигнал, что приводит к нарушению связи для всех абонентов этой пассивной оптической сети, причем найти поврежденное устройство очень трудно.

Миграция технологии. Через какое-то время наступит момент, когда необходимо будет обновить развернутое оборудование PON новой технологией, обеспечивающей большую полосу пропускания. Организации IEEE и ITU-T работают над стандартизацией требований для пассивных оптических сетей следующего поко-

ления со скоростью передачи данных 10 Гбит/с PON. Вероятнее всего эти решения не будут обратно совместимы с существующими технологиями PON (GPON или EPON).

В этом случае возможно два способа миграции с одной технологии PON на другую.

- Вывести из сервиса все оптическое дерево целиком, заменить все оконечные устройства, а затем вернуть структуру назад в сервис. Поскольку точки терминации оптической сети (ONT) обычно расположены на территории абонента, к которой у сервис-провайдера нет прямого доступа, этот процесс миграции может вызвать организационные проблемы и стать весьма трудоемким.
- Использовать уплотнение с разделением по длине волны, чтобы реализовать новую технологию PON с использованием тех же оптоволоконных линий, но на другой длине волны. Поскольку используемые в настоящее время приемники PON не поддерживают избирательность по длине волны, для этого необходимо перед началом миграции установить на всех оконечных устройствах фильтры длины волны.

Архитектура сети FTTH на базе коммутаторов так же представляет собой дерево, только в точках ветвления находятся активные устройства — коммутаторы Fast Ethernet и Gigabit Ethernet.

Это топология является более гибкой. Она позволяет реализовать режим полной дуплексной связи между узлом и любым из абонентов, а так же, при необходимости, режим широкого вещания. Связь между портом коммутатора и абонентом осуществляется по индивидуальной выделенной линии с высокой скоростью передачи данных.

Преимущества архитектуры Ethernet FTTH (P2P) перед пассивной оптической сетью

Решение Ethernet FTTH имеет множество преимуществ перед архитектурой на базе PON.

Практически неограниченная дискретная полоса пропускания. Прямая оптоволоконная линия может обеспечить практически неограниченную полосу пропускания, что позволяет достичь максимальной гибкости при развертывании сервиса в будущем, когда потребность в пропускной способности возрастет. Архитектура Ethernet FTTH позволяет сервис-провайдеру гарантировать каждому абоненту необходимую пропускную способность и создавать в сети профили полосы пропускания для каждого клиента индивидуально. Каждый частный или корпоративный пользователь может в любой момент получить симметричную полосу пропускания любой необходимой ему ширины.

Большой радиус действия. В типовых конфигурациях сетей доступа Ethernet FTTH применяются недорогие одноволоконные линии, использующие технологию 100BX или 1000BX, с заданным максимальным радиусом действия 10 км. Для работы на больших расстояниях имеются оптические модули, позволяющие увели-

чить мощность оптического сигнала, а также оптоволоконные пары с оптическими модулями, которые можно подключить к порту любого Ethernet-оборудования. В малонаселенных районах могут использоваться различные типы подключения Ethernet FTTH, которые не влияют на других абонентов на том же коммутаторе Ethernet.

Гибкий рост. Использовать порты на коммутаторе доступа Ethernet FTTH могут только те абоненты, которые оформили подписку у сервис-провайдера. В случае появления новых абонентов можно добавить дополнительные линейные карты Ethernet с высокой степенью модульности. Напротив, при использовании архитектуры на базе PON подключение первого абонента к оптическому дереву требует наличия наиболее дорогостоящего порта OLT, а при добавлении абонентов к тому же дереву PON стоимость подключения каждого абонента только увеличивается за счет приобретения ONT.

Миграция полосы пропускания. Поскольку одномодовые оптоволоконные линии не зависят от используемой технологии и скорости передачи данных, можно легко увеличить скорость для одного абонента, не влияя на работу других. Это означает, например, что абонент, использующий в настоящее время технологию Fast Ethernet, может в следующем году перейти на Gigabit Ethernet за счет простого переключения оптоволоконной линии абонента на другой порт коммутатора и замены только Ethernet-устройства в помещении абонента. Это изменение никак не повлияет на работу остальных абонентов сетей доступа Ethernet FTTH.

Отделение абонентских линий. Отделение абонентских линий — это свойство, присущее архитектурам Ethernet FTTH. Оно трудно реализуется в архитектуре пассивной оптической сети из-за общего характера передающей среды в дереве PON.

Безопасность. На сегодняшний день выделенная оптоволоконная линия является самой защищенной средой (на физическом уровне), особенно в сравнении с общими передающими средами. Кроме того, коммутаторы Ethernet, использующиеся в средах сервис-провайдеров, призваны обеспечить разделение физического уровня портов и логического уровня абонентов и имеют множество надежных функций защиты, которые в состоянии предотвратить практически все попытки вторжений.

Оборудование в помещении клиента. Архитектуры Ethernet FTTH предполагают использование на территории абонента простых устройств подключения к сети (customer premise equipment, CPE), обладающих достаточной функциональностью для обеспечения связи с сетью доступа и доставки всего спектра услуг каждому абоненту. Эти устройства Ethernet CPE стоят очень недорого и обычно размещаются в квартирах или домах абонентов. При использовании архитектуры на базе пассивной оптической сети (PON) устройство CPE (ONT) является неотъемлемой частью архитектуры PON, поскольку оно взаимодействует с другими устройствами при работе с общей передающей средой.

5.5 Радиодоступ

5.5.1 Общие принципы беспроводных сетей

Преимущества беспроводных технологий очевидны.

- Удешевление инфраструктуры в связи с отсутствием монтажа кабельных систем и активного оборудования. Стоимость самих работ, как правило, превышает стоимость кабелей.
- Удобство мобильного использования. Пользователь не привязан к рабочему месту и может свободно перемещаться в зоне обслуживания сети.

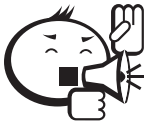
Технология широкополосного сигнала в беспроводных сетях

Приемлемые площадь покрытия и скорость передачи данных радиосети определяются прежде всего отношением сигнал/шум. Согласно теореме Шеннона скорость V [бит/с] не может превышать значения:

$$V = W \cdot \log_2 \left(\frac{S}{N} + 1 \right),$$

где W — ширина используемой полосы частот [Гц], S и N — значения уровней сигнала и шума в милливаттах соответственно.

Для того чтобы послать радиосигнал большой мощности в СВЧ-диапазоне, нужен дорогостоящий передатчик с усилителем и дорогостоящая узконаправленная антенна. Для того чтобы принять без помех сигнал малой мощности, также нужна аналогичная антенна и дорогой приемник с высокой чувствительностью. Превышение сигнала над шумами при использовании обычного «узкополосного» радиосигнала происходит за счет «вырезания» сигнала в частотной области и в пространстве. Картину усложняют еще и различные взаимные помехи между узкополосными сигналами большой мощности, передаваемыми близко друг от друга или на близких частотах. В частности, узкополосный сигнал может быть просто заглушен (случайно или намеренно) передатчиком достаточной мощности, настроившимся на ту же частоту.



Применяемый в беспроводных сетях принцип широкополосной связи ориентируется прежде всего не на превышение сигнала над шумами, а на способность оборудования выделять информацию за счет расширения спектра, т. е. введения некоторой избыточности.

Разработано два принципиально различающихся между собой метода использования такой широкой полосы частот:

- метод прямой последовательности (Direct Sequence Spread Spectrum — *DSSS*);
- метод частотных скачков (Frequency Hopping Spread Spectrum — *FHSS*).

Оба эти метода предусматриваются и стандартом 802.11 (Radio-Ethernet), а последний используется также и в технологии Bluetooth.

Метод прямой последовательности (DSSS)

Метод прямой последовательности (DSSS) можно представить себе следующим образом. Каждый передаваемый бит информации кодируется по заранее зафиксированному алгоритму в последовательность из N символов. При приеме полученная последовательность декодируется с использованием того же алгоритма, что и при ее кодировании. Другая пара приемник-передатчик может использовать другой алгоритм кодирования-декодирования, и таких различных алгоритмов может быть очень много.

Очевидно, для успешного приема информации приемнику необходимо знать следующее:

- кодовую последовательность, которая может насчитывать тысячи импульсов;
- фазу следования, которую невозможно определить, не зная самой последовательности.

Такие последовательности называют псевдошумовыми. Случайность их объясняется тем, что все вероятности значений последовательности распределены по определенным статистическим законам. Такой сигнал повторяется, но через большой относительно единичного элемента интервал времени (период повторения) так, что на одном периоде такую последовательность можно считать случайной, шумоподобной. Это позволяет получить максимум корреляционной функции между опорной и принятой последовательностями только при полном совпадении их вида и фаз. Отличие полезного «шума» от мешающего состоит в том, что на стороне и передатчика, и приемника последовательность известна и имеет один вид.

Первый очевидный результат применения этого метода — защита передаваемой информации от подслушивания («чужой» DSSS-приемник использует другой алгоритм и не сможет декодировать информацию не от своего передатчика). Но более важным оказалось другое свойство описываемого метода. Оно заключается в том, что благодаря *избыточности* передачи можно обойтись малым значением отношения сигнал/шум, приближающимся к единице, не увеличивая мощность передатчика.

Еще одно чрезвычайно полезное свойство DSSS-устройств заключается в том, что благодаря очень низкому уровню спектральной плотности *своего* сигнала, они практически не создают помех обычным радиоустройствам (узкополосным большой мощности), так как эти последние принимают широкополосный сигнал за шум в пределах допустимого. В другую же сторону — обычные устройства не мешают широкополосным, так как их сигналы большой мощности «шумят» каждый только в своем узком канале и не могут заглушить широкополосный сигнал весь целиком.

Таким образом, можно выделить положительные эффекты расширения спектра:

- помехозащищенность;
- не создаются помехи другим устройствам;
- конфиденциальность передач;
- экономичность при массовом производстве;
- возможность повторного использования одного и того же участка спектра.

Метод частотных скачков (FHSS)

При кодировке по методу частотных скачков (FHSS) вся отведенная для передач полоса частот подразделяется на некоторое количество подканалов (по стандарту 802.11 и Bluetooth этих каналов 79). Каждый передатчик в каждый данный момент использует только один из этих подканалов, регулярно перескакивая с одного подканала на другой. Стандарт 802.11 не фиксирует частоту таких скачков — она может задаваться по-разному в каждой стране. Эти скачки происходят синхронно на передатчике и приемнике в заранее зафиксированной псевдослучайной последовательности, известной обоим; ясно, что не зная последовательности переключений, принять передачу также нельзя.

Другая пара передатчик-приемник будет использовать и другую последовательность переключений частот, заданную независимо от первой. В одной полосе частот и на одной территории прямой видимости (в одной «ячейке») таких последовательностей может быть много. Ясно, что при возрастании числа одновременных передач возрастает и вероятность коллизий, когда, например, два передатчика одновременно перескочили на частоту №45, каждый в соответствии со своей последовательностью, и заглушили друг друга.

Метод частотных скачков, так же как и описанный выше метод прямой последовательности, обеспечивает конфиденциальность и некоторую помехозащищенность передач. Помехозащищенность обеспечивается тем, что если на какомнибудь из 79 подканалов передаваемый пакет не смог быть принят, то приемник сообщает об этом и передача этого пакета повторяется на одном из следующих (в последовательности скачков) подканалов.

С другой стороны, поскольку при использовании метода частотных скачков, в отличие от метода прямой последовательности, на каждом подканале передача ведется на достаточно большой мощности (сравнимой с мощностью обычных узкополосных передатчиков), про этот метод нельзя сказать, что он не мешает другим видам передач.

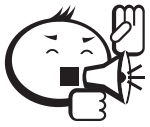
5.5.2 Стандарты IEEE 802.11 (Wi-Fi)

Для решения задач нестационарного беспроводного доступа в настоящее время наибольшую популярность приобрели сети на основе технологии «Wi-Fi», стандарты IEEE 802.11b и 802.11g с рабочей частотой 2.4 ГГц (11 Мбит/с у 802.11b, 22 Мбит/с у 802.11b+ против 54 Мбит/с у 802.11g). В это же семейство стандартов IEEE 802.11 входит и стандарт с индексом «a», работающий на частоте 5 ГГц (до 54 Мбит/с).

Благодаря меньшей стоимости и простоте лицензирования частот наибольшее распространение получила ветвь стандартов, совместимая с IEEE 802.11b. В соответствии с семиуровневой моделью OSI этот стандарт определяет физический и канальный уровни взаимодействия для беспроводных локальных сетей. Во многом на канальном уровне технология схожа с Ethernet, поэтому ее называют также беспроводным стандартом Ethernet. Наиболее важным отличием сети 802.11 от кабельных сетей являются ограничения по мощности передатчика и чувствительности приемника адаптера. В Ethernet все члены сети могут зафиксировать наличие коллизии в любой момент времени, в том числе и в момент передачи пакета. В беспроводной сети не все узлы могут находиться в зоне покрытия другой станции, поэтому

может возникнуть проблема «скрытого терминала». Пакеты в этом случае могут не мешать друг другу в местах передачи, но в месте приема может возникнуть коллизия, соответственно передатчик не может зафиксировать столкновение пакетов. Передающая станция 802.11 может убедиться в отсутствие коллизии только, если принимающая сторона ответит подтверждением о корректном приеме. В стандарте предусмотрена только полудуплексная связь, это обусловлено требованием простоты оборудования и ограничениями выделения рабочего частотного диапазона. Вся пропускная способность канала используется одной станцией в течение ограниченного стандартом интервала времени, поэтому скоростные характеристики сильно зависят от загруженности сети.

На физическом уровне в стандарте 802.11b используется технология DSSS (Direct Sequence Spread Spectrum — расширение спектра за счет прямой последовательности), где каждый бит кодируется определенной последовательностью (чип-кодом), принятой в одной локальной сети. В стандартах 802.11a используется модуляция OFDM (Orthogonal Frequency Division Multiplexing — мультиплексирование с ортогональным разделением частот). В 802.11g используется последний вид расширения спектра, но для совместимости с более старым 802.11b может применяться и DSSS.



Существуют два вида архитектур, применяемых в 802.11:

- инфраструктурная сеть, или BSS (Basic Service Set — базовый служебный комплект), изображена на рисунке 5.19;
- независимая сеть, «ad-hoc», или IBSS (Independent Basic Service Set — независимый базовый служебный комплект), изображена на рисунке 5.20.

Наиболее часто используется архитектура BSS с центральным элементом — точкой доступа, ТД (AP — Access Point). ТД представляет собой беспроводной концентратор, который можно подключить к обычной проводной сети, при этом для пользователя как мобильного, так и стационарного не существует различий в работе с сетевыми приложениями. Как видно из рисунка, используется топология «звезда», и весь трафик, например от станции А к станции Б, в такой сети должен проходить через ТД, т. е. каждый кадр пересылается по радиоканалу дважды. Такой недостаток несущественен, если беспроводная сеть является средством доступа к более крупной проводной сети. Кроме того, такая структура решает проблему «скрытого терминала», т. к. все узлы находятся в зоне видимости ТД.

Полудуплексный Ethernet использует принцип CSMA (CSMA — Carrier Sense Multiple Access) для доступа терминалов к среде, беспроводные стандарты 802.11 изначально ориентировались на полудуплексную связь, более простую в аппаратном и частотном обеспечении, поэтому технология «Wi-Fi» использует именно этот принцип. Это значит, что любой из участников сети может получить доступ к среде передаче данных, предварительно определив, что канал не занят. Однако каким образом передающие устройства беспроводных адаптеров определяют факт «столкновения пакетов» друг с другом? В случае использования CSMA/CD

коллизию можно было бы обнаружить лишь на стороне приемника. В спецификации стандарта 802.11 указывается, что физический уровень наблюдает за уровнем радиосигнала, чтобы определить, не занят ли канал другой станцией. Но тогда одновременно с передатчиком в адаптере должен работать специальный приемник для обнаружения коллизий.

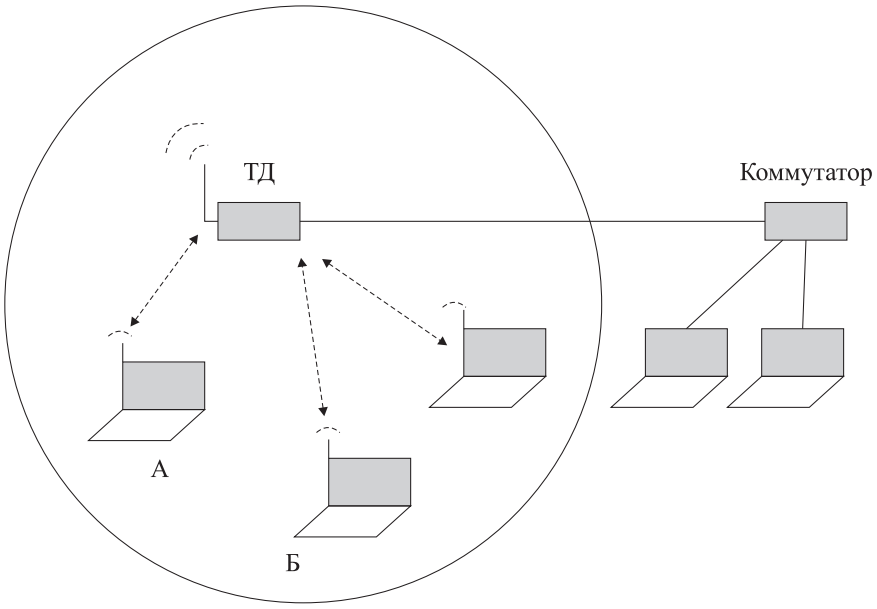


Рис. 5.19 – Архитектура BSS в беспроводных сетях 802.11

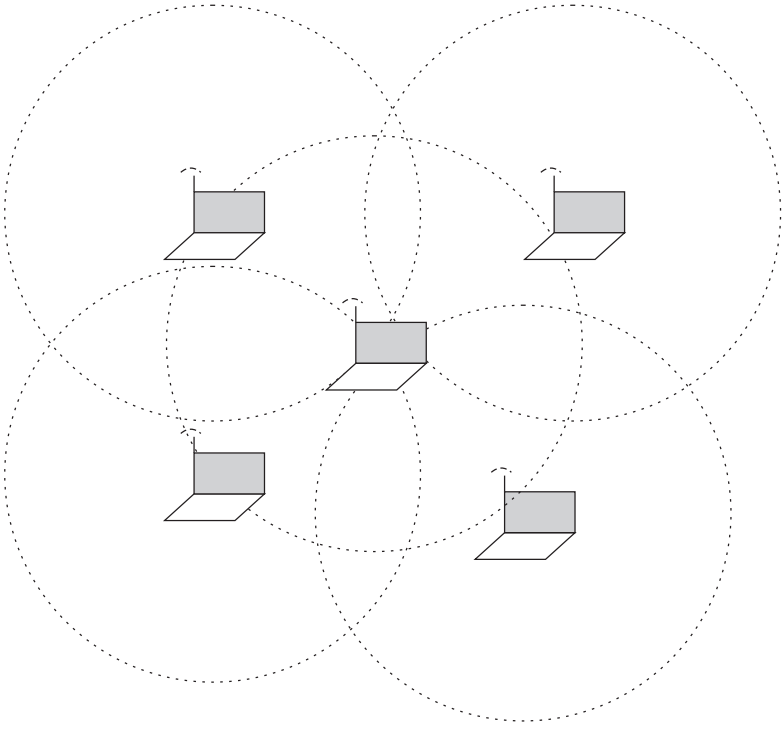
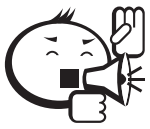


Рис. 5.20 – Архитектура IBSS в беспроводных сетях 802.11



Проблема обнаружения коллизий была решена при помощи видоизмененного принципа множественного доступа.

Допустим, станция А и В имеют информацию для Б (рис. 5.21). Каждое из устройств определяет, занята ли среда. Если эфир свободен, то станция А выжидает время интервала между кадрами DIFS (Distributed Inter Frame Space). Если канал оказывается свободным в течение этого времени, то станция выжидает короткий случайный интервал, после чего может послать кадр. Интервал случайной длительности помогает избежать ситуации, когда несколько узлов начинают передачу одновременно. ТД доступа, как и ее проводной аналог, просто транслирует полученные пакеты. Получив корректный кадр, принимающая станция Б ждет в течение короткого периода времени SIFS (Short Inter Frame Space — короткий межкадровый интервал), затем посылает кадр подтверждения (ACK — aknowlegement, подтверждение). Если подтверждение не пришло, станция А считает, что пакет потерян, и переходит к процедуре отката после коллизии аналогично Ethernet. За время общения двух станций — NAV (Network Allocation Vector) другие члены сети (В) находятся в режиме молчания. Этот интервал вычисляется на основе значения длины, которое содержится в служебных полях кадра.

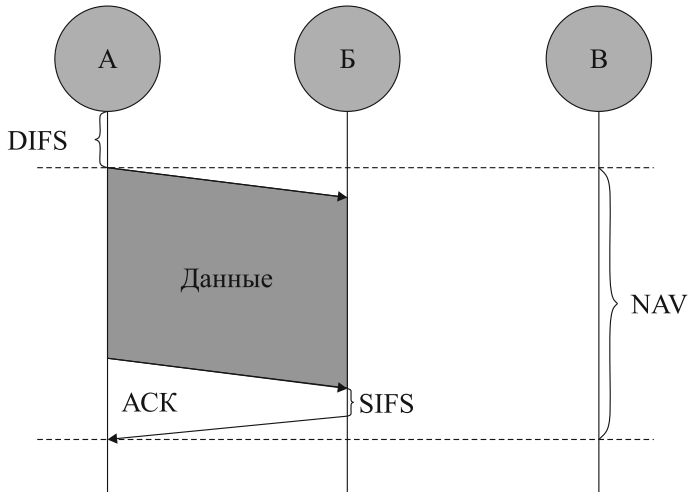


Рис. 5.21 – Принцип CSMA в сетях 802.11

Станции могут группироваться по принципу ad-hoc — сеть без центрального элемента, как показано на рисунке 5.20. В этом случае станции устанавливают связь друг с другом, используя топологию полносвязанной сети. Схема информирования о коллизиях эффективна для архитектуры BSS, но для независимой сети ad-hoc (IBSS) существует проблема скрытого терминала, которая решается при помощи принципа предотвращения коллизий.

Для доступа к среде передачи данных используется метод коллективного доступа с обнаружением несущей и предотвращением коллизий CSMA/CA (Carrier-SenseMultipleAccess/CollisionAvoidance).

Перед тем как послать данные, станция сначала отправляет специальное сообщение, называемое RTS (ReadyToSend), которое трактуется как готовность данного узла к отправке данных. RTS-сообщение содержит информацию о продолжительности предстоящей передачи и адресате и доступно всем узлам в сети. Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция, получив сигнал RTS, отвечает посылкой сигнала CTS (ClearToSend), соответствующего готовности станции к приему информации. После этого передающая станция посылает пакет данных, а приемная станция должна передать кадр АСК, подтверждающий безошибочный прием. Если АСК не получен, попытка передачи пакета данных будет повторена. С использованием такого четырехэтапного протокола передачи данных реализуется регламентирование коллективного доступа с минимизацией вероятности возникновения коллизий (рис. 5.22).

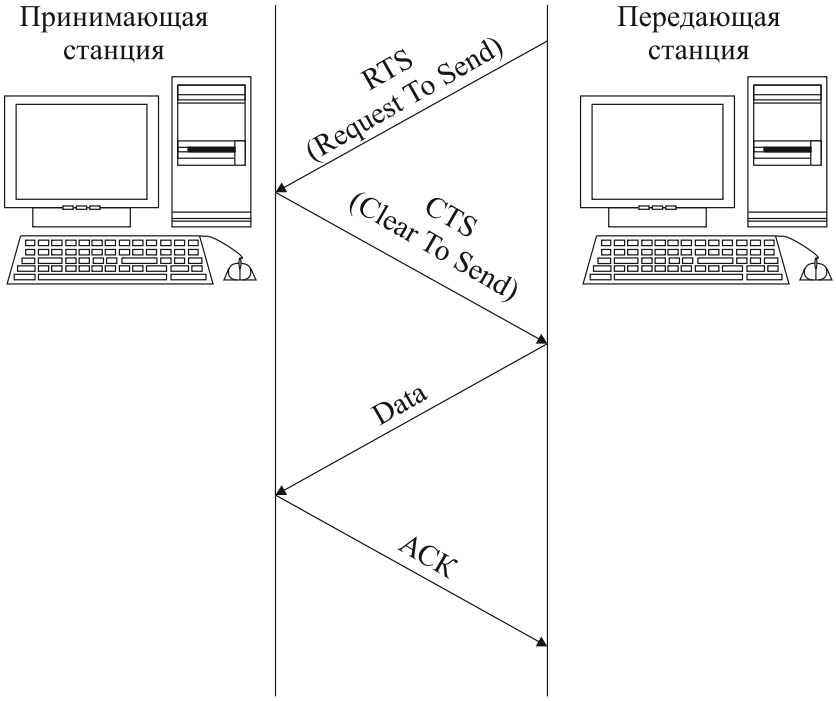


Рис. 5.22 – Технология CSMA/CA

Каждый пакет данных снабжается контрольной суммой CRC, что гарантирует обнаружение «битых» кадров при приеме. Пакетная фрагментация, определяемая в стандарте, предусматривает разбивку большого пакета данных на малые порции. Такой подход позволяет снизить вероятность повторной передачи кадра данных, поскольку с увеличением размера кадра возрастает и вероятность ошибки при его передаче. Если же переданный кадр оказался «битым», то в случае малого размера кадра передающей станции придется повторить только малый фрагмент сообщения.

Контрольные вопросы по главе 5

1. Охарактеризуйте мини-АТС как узел доступа.
2. Назовите варианты реализации DSL-модемов.
3. Приведите целесообразность применения ассиметричного режима в модемах ADSL.
4. В чем отличие пассивных и активных оптических сетей доступа?
5. В каком диапазоне длин волн работает пассивный Gigabit Ethernet (GPON)?
6. Назовите преимущество сетей радиодоступа.
7. Какое предельное соотношение сигнал/шум можно реализовать в системах связи с шумоподобными сигналами?

Глава 6

ИНТЕГРАЦИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И УСЛУГ

6.1 Общие соображения

Интеграция услуг заключается в том, что к абоненту по одной линии связи приходят электрические сигналы разных служб. Здесь с помощью устройства распределения услуг они разделяются по соответствующим терминальным устройствам (телефонный аппарат, модем, телевизионный приемник и т. д.). Самым радикальным случаем является тот, когда по линии связи одновременно приходят услуги телефонии, телевидения и передачи данных [1, 4, 5]. Однако на настоящий момент для массового абонента такого сервиса еще нет, и на практике применяют попарную интеграцию. Рассмотрим развитие услуг и возможные варианты интеграции с помощью диаграммы (рис. 6.1).

Наиболее просто решаются задачи объединения двух услуг. Назовем это первым уровнем интеграции. Здесь с технической точки зрения проще интегрировать телефонию и передачу данных. В соответствии с диаграммой возможны и развиваются три варианта.

1. Аналого-цифровая интеграция, когда канал тональной частоты (телефонный канал), используя ЧРК, объединяется с цифровым каналом передачи данных. Наиболее распространена технология ADSL.
2. Цифровая интеграция, в которой на принципах ВРК объединяются цифровые потоки телефонии и передачи данных — это технологии ISDN BRI и PRI.
3. Интеграция на базе IP-протоколов, когда речь и данные передаются в виде пакетов.

Кроме этого, реализуются и другие варианты интеграции 1 уровня. Наиболее распространена схема объединения сигналов аналогового кабельного телевидения

и передачи данных (доступ в Интернет). Это не означает, что не появятся другие варианты интеграции 1 уровня, например «Речь-Телевидение», в аналоговом, цифровом или комбинированном исполнении.

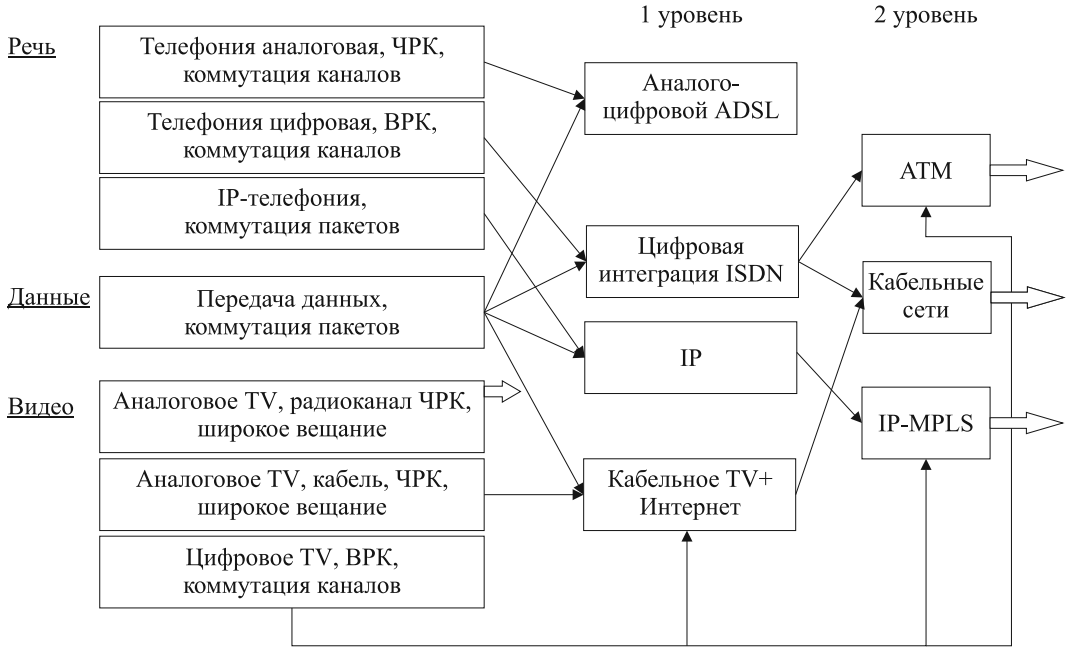


Рис. 6.1 – Развитие и интеграция услуг

Если технологии первого уровня интеграции находятся на этапе массового внедрения, то полная интеграция (2 уровень) испытывает стадию экспериментальных исследований и опытного внедрения. В настоящее время наибольшую известность имеют технологии:

- ATM — специально разработанная для полной интеграции, способная обеспечить разные уровни сервиса, высокие скорости передачи и другие достоинства цифровых технологий. Основным ее недостатком является высокая стоимость оборудования, что сдерживает широкое внедрение;
- IP MPLS — эволюционирует от услуг по передаче данных, постепенно включая в себе телефонию, а затем и телевидение. Такой подход является более рациональным и менее затратным, хотя по техническим характеристикам IP-технологии уступают ATM. Более совершенным вариантом технологии IP MPLS является NGN (Next Generation Networks);
- менее прогрессивным является способ интеграции 2 уровня на базе кабельного телевидения, так как в его основе пока лежат методы передачи аналоговых сигналов и ЧРК. В то же время сети кабельного телевидения хорошо развиты, и не исключено, что на первом этапе они и будут основой для массовой услуги.

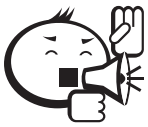
Все описанные выше тенденции развития телекоммуникаций активно реализуются в настоящее время с внедрением:

- волоконно-оптических линий связи (ВОЛС) и систем передачи, имеющих реальную пропускную способность при передаче цифровых сигналов в несколько сотен гигабит в секунду в одном волокне;

- цифровых систем коммуникации и распределения трафика с использованием технологий коммутации каналов и коммутации пакетов. Число абонентских линий в цифровых коммутационных станциях достигает 200–300 тысяч;
- систем кабельного телевидения с числом телевизионных программ до 100 и доступом в Интернет со скоростью до 40 Мбит/с;
- систем IP-телефонии с пакетной передачей речи в IP-сетях, в которых себестоимость услуги междугородной и международной телефонии снижается в несколько (3–5) раз без заметного ухудшения качества;
- сотовых систем связи и многих других достижений.

6.2 Интеграция услуг в сетях передачи данных

Рассмотрим теперь особенности передачи трафика реального времени (телефония, видео и т. п.) в СПД.



В таблице 6.1 приведены требования, предъявляемые к основным характеристикам передачи трафика телефонии и трафика передачи данных.

Таблица 6.1 – Требования к телекоммуникационным системам

Услуги	Характеристики		
	Допустимая задержка, мс	**Вероятность потери пакета**	**Скорость передачи, кбит/с**
Речь/телефон	$\leqslant 150$	0.05–0.1	6–8
Данные	Не критично	10^{-2}	30–100 000

Из нее видно, насколько эти требования противоречивы. Если для передачи речи задержка (время передачи от абонента к абоненту) не должна превышать 150 мс, то для передачи данных она не существенна. Это требование является самым серьезным для пакетной телефонии, поскольку по вероятности ошибки и скорости передачи требования к речевому трафику намного мягче.

Поскольку технологии коммутации пакетов разнообразны, то и способов пакетной телефонии тоже несколько:

- V_0 FR (голос поверх Frame Relay);
- V_0 IP (IP-телефония);
- V_0 ATM (голос поверх ATM).

Наибольшее распространение получила IP-телефония, технологии которой непрерывно развиваются.

Основными проблемами, которые приходится решать при внедрении IP-телефонии, являются:

1. Удовлетворение условий по задержке ($\tau_з$ < 150 мс). Эта проблема стоит более остро, чем в обычной телефонии по следующим причинам:

- большая задержка в узлах сети (маршрутизаторах и коммутаторах), которая обусловлена временем ожидания пакета в очереди, временем записи и временем считывания;
- влияние операционной системы маршрутизатора на скорость обработки речевых сигналов, на установление соединения, на доступ к IP-сети;
- влияние кодера речи, который в процессе кодирования должен записать фрагмент речи (совокупность отсчетов) и проанализировать его с точки зрения возможности сжатия информации.

2. Сигнализация. Установление соединения в системах IP-телефонии предполагает преобразование номера телефонной сети в IP-адрес.
3. Качество обслуживания. Скорость установления соединения, ошибки при передаче пакетов, переменная задержка при передаче.

Наиболее проработана технология IP-телефонии по рекомендации ITU-T H.323. Схема сети IP-телефонии по этой рекомендации приведена на рисунке 6.2.

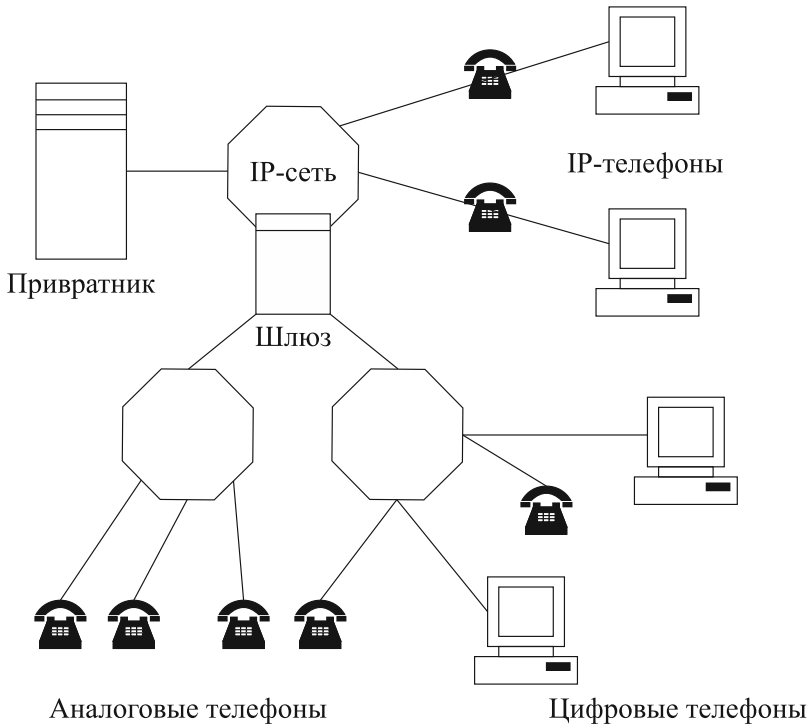


Рис. 6.2 – Архитектура сети H.323

Здесь возможны следующие варианты:

- общение IP-телефонных абонентов только через IP-сеть между собой (модель «компьютер — компьютер»);
- общение IP-телефонных абонентов с абонентами ТФОП или ISDN через шлюз (модель «компьютер — телефон»);
- общение абонентов, принадлежащих к разным узлам ТФОП через IP-сеть и совокупность шлюзов (модель «телефон — телефон»).

Рассмотрим основные элементы сети: IP-телефон или терминал H.323 (рис. 6.3).

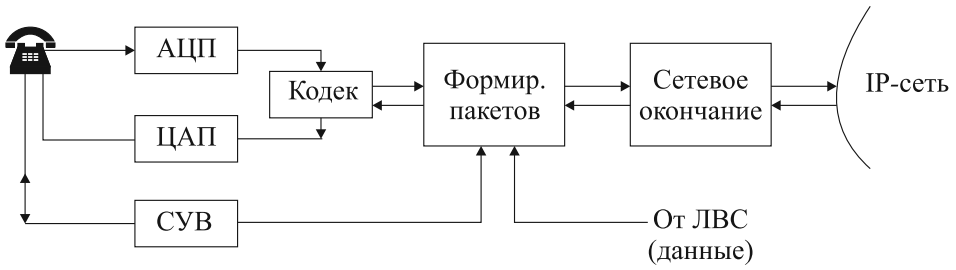


Рис. 6.3 – Структура IP-телефона

Он включает в себя телефонную трубку (микрофон + динамик), устройства аналого-цифрового преобразования, кодек для сжатия цифрового сигнала со скоростью 64 Кбит/с до значений 6–16 Кбит/с, устройство пакетизации/депакетизации и сетевое окончание. Наряду с речевыми пакетами IP-телефон передает сигналы управления и взаимодействия (СУВ), с помощью которых обеспечивается регистрация терминала у привратника, установление и завершение соединения, открытие разговорного канала и техобслуживание.

Шлюз H.323 — обеспечивает передачу речевого и сигнального трафика и трафика передачи данных по IP-сети, причем на вход шлюза могут поступать как сигналы терминалов H.323, так и сигналы аналоговой телефонии (ТФОП) и цифровой (ISDN). В двух последних случаях он преобразует речевые сигналы к виду, пригодному для передачи по IP-сети.

Привратник — это специализированный сервер, который выполняет следующие функции:

- регистрация терминалов и других устройств;
- контроль доступа пользователей к услугам;
- преобразование телефонного номера или другой адресной информации в IP-адрес;
- контроль, управление и резервирование пропускной способности сети.

Основным достоинством IP-телефонии, особенно в схеме «телефон — телефон», является существенное снижение затрат на передачу трафика (от 3 до 10 раз). Это позволяет значительно уменьшить тарифы при повременном учете длительности разговоров (междугородные и международные).

Другие, не менее существенные преимущества IP-телефонии заключены в интеграции трафика и услуг телефонии и передачи данных. Эти потенциальные качества только начинают осмысливаться, и у них большое будущее.

К недостаткам IP-телефонии относится ухудшение качества за счет задержек и пропадания пакетов. Для борьбы с этим принимаются такие меры:

- установление приоритетов для речевого трафика;
- недогрузка каналов в IP-сети;
- снижение числа промежуточных узлов (хопов) на пути прохождения трафика IP-телефонии;

- применение механизмов обеспечения качества (QoS) в IP-сетях, таких как RSVP, Diff — Serv, MPLS.

6.3 Сети MPLS и NGN

Технология MPLS (Multi Protocol Label Switching) — это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. Повышенная скорость коммутации определяется тем, что вместо анализа достаточно длинного сетевого (IP) или MAC-адреса в MPLS направление пакета по маршруту осуществляется после считывания более короткой метки. Эта метка не заменяет IP- и MAC-адрес, а добавляется к ним (рис. 6.4).

Рис. 6.4 – Расположение метки

Многопротокольный характер метки означает, что MPLS работает по принципу инкапсуляции и может транспортировать множество других протоколов (рис. 6.5).

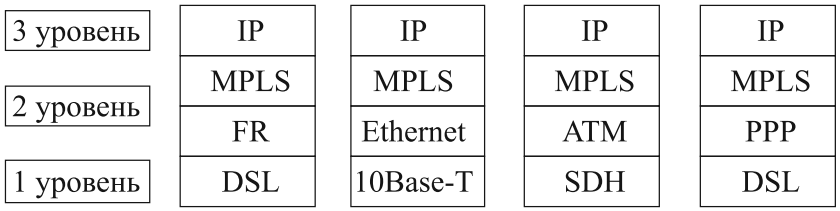


Рис. 6.5 – Место MPLS в эталонной модели BOC и в технологии IP

Еще одним важным достоинством MPLS является возможность обеспечения QoS. Для этого метки наделяются признаком класса обслуживания. FEC (Forwarding Equivalence Class). Более того, вводится целый стек (совокупность) меток, чтобы можно было отделить функции передачи и функции сервиса.

Фрагмент сети IP-MPLS представлен на рисунке 6.6.

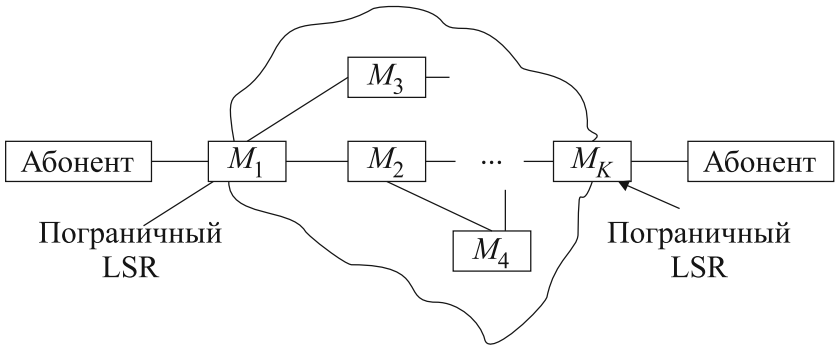


Рис. 6.6 – Сеть MPLS-IP

Сеть состоит из маршрутизаторов M_i с коммутацией меток LSR — Label Switching Router, которые направляют трафик по предварительно проложенным путям

с коммутацией меток. Метка присваивается каждому пакету и содержит информацию о пути следования и о классе обслуживания. Содержание метки действует только на участке между двумя соседними LSR. LSR — это сочетание обычного маршрутизатора и высокоскоростного коммутатора. Маршрутизатор определяет топологию сети по принятым алгоритмам (OSPF, BGP и др.), выбирает рациональные маршруты, а коммутатор обеспечивает передачу пакетов с использованием меток и упрощенных локальных таблиц коммутации.

Сеть MPLS делится на две функционально различные области — ядро и граничную область. Маршрутизаторы ядра занимаются только передачей пакетов. Все функции классификации пакетов по различным FEC, фильтрации, выравнивания нагрузки, управления трафиком берут на себя пограничные LSR. Поэтому объемные и интенсивные вычисления приходятся на граничную область, а высокоскоростная коммутация на ядро.

Обеспечение QoS с помощью классов сервиса FEC позволяет передавать пакеты разных классов по разным путям и с разными приоритетами. Кроме этого, механизм MPLS позволяет обеспечить дополнительные функции QoS путем сочетания с другими механизмами обеспечения качества. Например, это механизм RSVP — Resource Reservation Protocol. RSVP — это протокол сигнализации, который обеспечивает резервирование ресурсов, таких как гарантированная пропускная способность канала, предсказуемая задержка, предельный уровень ошибок и потерь. Протокол запрашивает для своего абонента у маршрутизаторов сети необходимый уровень QoS и при наличии требуемого ресурса гарантирует данную услугу. В случае MPLS метка будет учитывать результаты RSVP переговоров и обеспечит данный качественный маршрут. Таким образом, MPLS управляет качеством услуги в транспортной сети, а RSVP в сети доступа.

Нетрудно увидеть, что MPLS-IP и ATM — две остро конкурирующие технологии. Пока соревнование выигрывает MPLS по следующим причинам:

1. Сеть IP — уже является глобальной и надстройка в виде MPLS легко внедряется и хорошо масштабируется в магистральных сетях.
2. Оборудование ATM значительно дороже, особенно для крупных узлов.
3. Несмотря на то, что в ATM изначально решены многие противоречия телекоммуникационных систем по скорости, задержкам, QoS, технология IP-MPLS успешно их решает с применением механизмов MPLS, RSVP и других.

NGN — Next Generation Networks — сети следующего поколения. К настоящему времени сложилось следующее определение NGN: гетерогенная мультисервисная сеть, обеспечивающая передачу всех видов медиатрафика и распределенное предоставление неограниченного спектра телекоммуникационных услуг, с возможностью их добавления, редактирования, распределенной тарификации. Сеть поддерживает передачу разнородного трафика с различными требованиями к качеству обслуживания с минимальными затратами.

Как видим, преодоление многих противоречий, описанных выше, может быть реализовано в сетях NGN.

В *основе концепции NGN* лежат следующие положения:

- мультисервисное обслуживание абонентов (интеграция услуг телефонии, видео и передачи данных);

- поставщики услуг должны быть независимы от операторов связи, любая новая услуга должна быть доступна любому абоненту;
- транспортная сеть должна быть построена по технологии коммутации пакетов, система коммутации является распределенной;
- сеть доступа должна быть широкополосной и включать в себя все перспективные технологии (Ethernet, V.35 + PPP, PDH, ATM и др.);
- управление качеством предоставления услуг.

В связи с этим можно сеть NGN представить в виде следующей структуры (рис. 6.7). Здесь ядро транспортной сети образует сеть передачи данных, которая через медиашлюзы соединена с телефонной сетью общего пользования и мобильными сетями. Назначение медиашлюзов — преобразование информационных потоков к виду, удобному для передачи по сети передачи данных.

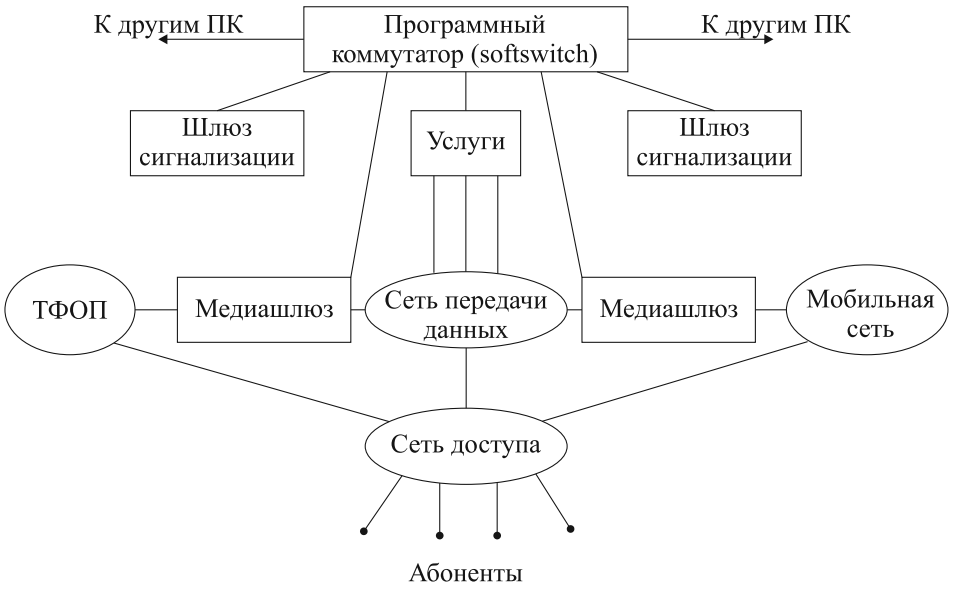


Рис. 6.7 – Структура сети NGN

Наряду с этими шлюзами существуют шлюзы сигнализации, которые согласуют процедуры установления соединения абонентов между собой и процедуры получения абонентами других различных услуг. Всем этим управляет специальный программный коммутатор (softswitch), который регулирует установление соединения и обеспечивает подключение абонента к необходимой ему услуге.

В качестве прообраза NGN сетей чаще всего используют IP-сети. Для того чтобы это увидеть, изобразим процессы в NGN с помощью системы уровней (рис. 6.8). Здесь же приведем структуру уровней стека протоколов TCP/IP.

Здесь, как и в NGN, так и в TCP/IP на физическом и канальном уровнях допускаются любые интерфейсы и протоколы. Сетевой уровень обеспечивает передачу пакетов с помощью маршрутных таблиц. На четвертом (транспортном) уровне к известным протоколам гарантированной доставки пакетов (TCP) и негарантированной доставки (UDP) добавляется протокол RTP (Realtime Transport Protocol), обеспечивающий доставку пакетов в реальном масштабе времени. Это необходимо при передаче голосового трафика (IP-телефония) и изменяющегося во времени

изображения (телевидение). Основная функция RTP — сглаживание джиттера (изменения задержки сигнала). Как правило, RTP работает совместно с протоколами UDP и RTCP.

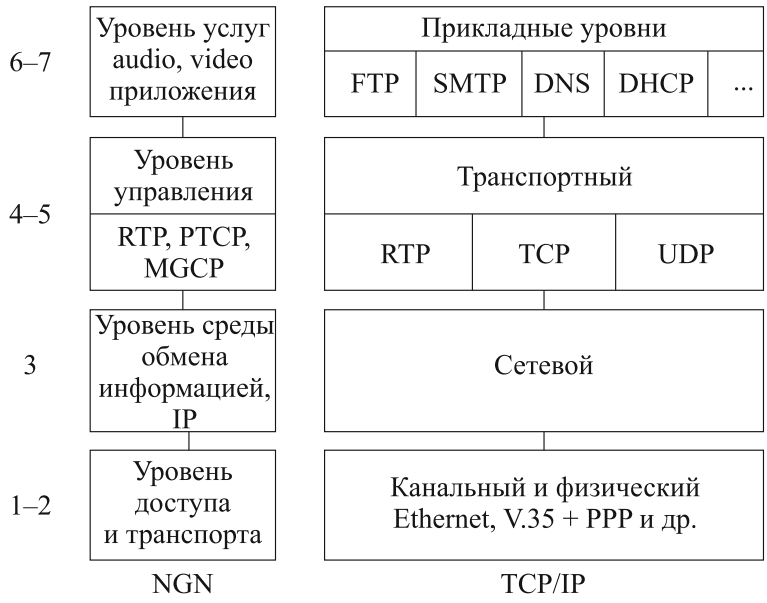


Рис. 6.8 – Структура уровней NGN и TCP/IP

Протокол RTCP предназначен для контроля качества прохождения пакетов (сбор статистики о задержке пакета, джиттере, количестве и доле потерянных пакетов).

На уровне управления NGN, помимо RTP, введены и другие протоколы. Например, MGCP (Media Gateway Control Protocol) — назначение которого — управление шлюзами со стороны программных коммутаторов.

Для коммутации мультимедийных приложений через IP-сети разработаны специальные протоколы H.323, SIP, MGCP, MEGACO и др. Протокол H.323 реализуется в IP и осуществляет связь по цепочке: абонент → медиашлюз → IP-сеть → → программный коммутатор (привратник) → IP-сеть → медиашлюз → абонент. Назначение программного коммутатора — трансляция адресов, идентификация и авторизация абонентских терминалов, сбор статистики и тарификация.

В последнее время протокол H.323, который является достаточно сложным, заменяется протоколом SIP (Session Initiation Protocol). Он базируется на протоколе HTTP, работает поверх протокола UDP. Элемент сети на базе протокола SIP изображен на рисунке 6.9. Передача информации (телефония, данные, видео) осуществляется после установления соединения. Для этого абонент А (клиент) обращается с запросом к своему серверу, назначение которого принимать и транслировать запросы и возвращать ответы. Запрос транслируется на прокси-сервер, который устанавливает местоположение абонента В с помощью сервера местоопределения и транслирует запрос абоненту В через его серверы.

В другом варианте связи местоположение абонента В с помощью сервера переадресации сообщается непосредственно абоненту А и передача информации ведется непосредственно между абонентами, минуя прокси-серверы.

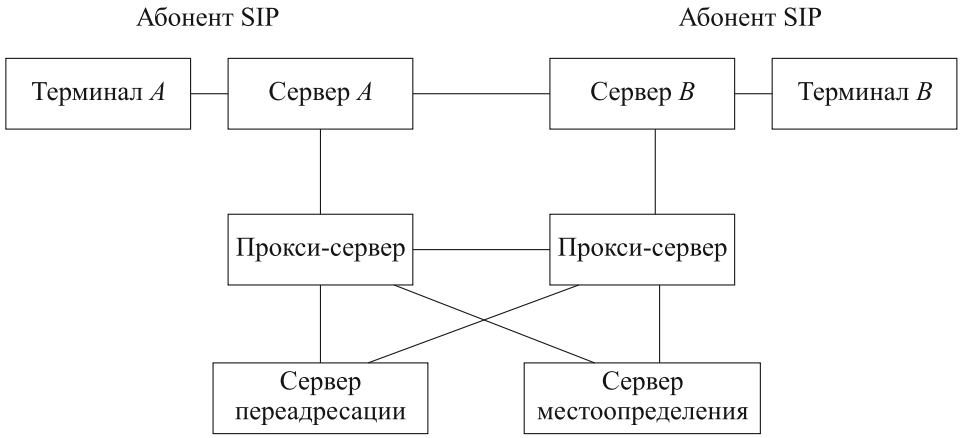


Рис. 6.9 – Элемент SIP-сети

Внедрение NGN предполагается эволюционным путем, так как на сетях электросвязи используется много коммутационных станций, работающих по технологии коммутации каналов. В сетях доступа также много терминального оборудования и оборудования узлов, не исчерпавших свой ресурс. Поэтому один из возможных сценариев перехода к NGN в городских телефонных сетях следующий:

1. Вначале создается междугородний узел NGN (IP-телефония). Одновременно функционирует «классическая» АМТС, работающая по технологии коммутации каналов. Распределение нагрузки между ними осуществляет специальный сервер.
2. На ряде АТС создаются узлы NGN, которые реализуют режим коммутации пакетов. Линии, соединяющие эти узлы, работают по протоколам IP или родственным им протоколам.
3. Технология NGN внедряется на всей сети.

Помимо IP-телефонии перспективными направлениями NGN являются конвергенция проводной и беспроводной связи, конвергенция телекоммуникаций и информационных технологий.

Контрольные вопросы по главе 6

1. Объясните, почему различные требования предъявляются к задержке сигналов в телефонных сетях и сетях передачи данных.
2. Назовите основные механизмы задержки сигнала в системах IP-телефонии.
3. Какие меры принимаются для улучшения качества передачи речи в IP-телефонии?
4. Зачем применяются метки в технологии MPLS?
5. Какая технология коммутации используется в системах NGN?

ЗАКЛЮЧЕНИЕ

Перспективы развития телекоммуникационных систем и сетей передачи данных заключаются в дальнейшем развитии цифровых методов передачи, расширении зоны применения волоконной оптики в сетях доступа, широком применении технологий коммутации пакетов и интеграции услуг.

В области волоконно-оптических линий связи перспективно спектральное уплотнение (ЧРК), когда в одном волокне передаются сигналы от нескольких независимых световых источников. В области радиосвязи интенсивно применяются технологии коммутации пакетов. Быстро развиваются технологические и промышленные сети (Wi-Fi, Wi-Max, стандарт 80215.4), мобильные сети четвертого поколения, технологии OFDM. В области пакетных технологий доминирующее место занимают IP-системы (IP-телефония, IPTV, сети с интеграцией услуг NGN).

ЛИТЕРАТУРА

[1] Олифер В. Г. Компьютерные сети / В. Г. Олифер, Н. Г. Олифер. — СПб. : Питер, 2010.

[2] Агеев Е. Ю. Локальные компьютерные сети: учеб. пособие [Электронный ресурс] / Е. Ю. Агеев. — 2012. — 105 с. — URL: http://edu.tusur.ru/training/publications/2038 (дата обращения: 14.01.2015).

[3] Максимов Н. В. Компьютерные сети : учеб. пособие / Н. В. Максимов, И. И. Попов. — М. : Форум, 2005 ; М. : ИНФРА-М, 2005. — 335 [1] с. : ил, табл.

[4] Основы построения систем и сетей передачи информации : учеб. пособие для вузов / В. В. Ломовицкий [и др.]. — М. : Горячая линия-Телеком, 2005. — 384 с.

[5] Илюхин Б. В. Сетевые информационные технологии : учеб. пособие / Б. В. Илюхин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники ; Кафедра радиоэлектроники и защиты информации. — Томск : ТМЦДО, 2005. — 229 с.

[6] Карасев А. П. Проектирование компьютерной сети : учеб. пособие / А. П. Карасев. — М. : Издательство Московского государственного открытого университета, 2010. — 150 с.

[7] Крук Б. И. Телекоммуникационные системы и сети / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов. — М. : Горячая линия-Телеком, 2003. — Т. 1.

[8] Кульгин М. Технологии корпоративных сетей / М. Кульгин. — СПб. : Питер, 1999.

[9] Убайдуллаев Р. Р. Волоконно-оптические сети / Р. Р. Убайдуллаев. — М. : Эко трендз, 2000.

[10] Гук М. Аппаратные средства локальных сетей / М. Гук. — СПб. : Питер, 2003. — 576 с.

[11] Фейт С. TCP/IP: Архитектура, протоколы, реализация / С. Фейт. — М. : Лори, 2000. — 424 с.

[12] Ногл М. TCP/IP. Иллюстрированный учебник / М. Ногл. — М. : ДМК Пресс, 2001. — 480 с.

[13] Гасымов И. Архитектура оптических сетей [Электронный ресурс] / И. Гасымов. — URL: http://www.uran.donetsk.ua/~masters/2013/fkita/bahrullo/library/cisco.htm (дата обращения: 02.02.2015).

ГЛОССАРИЙ

Ethernet — технология передачи в основной полосе и случайный доступ к среде. Передача в прямой полосе — прямая (немодулированная) передача данных по сети. Способ передачи, при котором цифровой сигнал направляется непосредственно в канал связи без всякой модуляции т. е. несущая частота отсутствует.

FTTH (Fiber to the Home) — оптоволоконные сети доступа. В них оптоволокно доходит либо до дома (узел размещается в цокольном этаже FTTB (Fiber to the Building)), либо до квартиры.

GPON (Gigabit PON) — перспективный стандарт PON ITU G.984 (2005).

MPLS (Multi Protocol Label Switching) — это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток.

NGN (Next Generation Networks) — сети следующего поколения. Гетерогенная мультисервисная сеть, обеспечивающая передачу всех видов медиатрафика и распределенное предоставление неограниченного спектра телекоммуникационных услуг, с возможностью их добавления, редактирования, распределенной тарификации.

PON (Passive optical network) — пассивные оптические сети, работающие по технологии «дерево» на базе пассивных оптических разветвителей.

RIP (Routing Information Protocol) — этот протокол анализирует маршрут на основе вектора расстояния, когда каждому хопу присваивается вес (обычно 1). Для каждого пути все веса суммируются, а затем из всех путей выбирается маршрут с наименьшей метрикой.

TCP (Transmission Control Protocol) — протокол с управлением передачи, принципиально отличающийся от UDP, поскольку он вначале устанавливает виртуальное соединение между двумя абонентами, а потом по этому пути передает их пакеты наряду с пакетами других абонентов. Связь по TCP — дуплексная и без ошибок. По сути дела, протокол TCP позволяет в стеке TCP/IP совмещать две разные технологии: датаграммную и виртуального соединения.

UDP (User Datagram Protocol) — протокол негарантированной доставки, который обеспечивает передачу пакетов датаграммным способом и по сути является продолжением протокола IP.

V.35 — протокол, регламентирующий постоянное модемное соединение в синхронном режиме передачи по выделенной линии.

Автономная система (АС) — подключенный сегмент сетевой топологии, состоящий из набора подсетей и взаимодействующий через набор маршрутизаторов. Каждая автономная система имеет свой уникальный номер (сетевой адрес или префикс) и находится под единым управлением. Типичной автономной системой является сеть крупной компании или провайдера сетевых услуг.

Адреса аппаратные — уникальные цифровые адреса сетевых карт, которые задаются их производителями. Эти адреса функционируют на канальном уровне ЭМВОС и непосредственно могут работать только в небольших локальных сетях. Для адресации в больших сетях они не применяются, так как не обладают свойством иерархичности. Поэтому таблицы, составляемые из таких адресов, очень громоздки и сложны для администраторов сетей.

Адреса числовые (сетевые) — это тоже уникальные цифровые адреса, но они присваиваются не сетевым картам, а пользователям единой международной организацией IANA — Internet Assigned Numbers Authority — комиссией по константам Интернет. Система регистрации описана в документе RFC2050, а деятельность IANA в RFC1700. В этой системе задается номер сетевого узла в старших битах и номер хоста в младших битах.

Адресация в ЛВС подразумевает использование типичных для сетевых окружений адресов (MAC-адресов).

Виртуальные частные сети (VPN — Virtual Private Networks) организуют потоки данных одного предприятия, которые существуют в открытой сети с коммутацией пакетов и в достаточной степени защищены от влияния потоков данных других абонентов этой сети.

Глобальные вычислительные сети (ГВС) — сети, охватывающие значительные территории: регион, страна, значительная часть земного шара.

Интеграция услуг заключается в том, что к абоненту по одной линии связи приходят электрические сигналы разных служб.

Инкапсуляция протоколов — процедура добавления к пакету высшего уровня заголовка более нижнего уровня.

Коммутатор — это многопортовое устройство, содержащее коммутационную матрицу, входные и выходные порты и процессорный блок.

Компьютерная сеть — система распределенной обработки информации, состоящая из территориально разнесенных компьютеров, взаимодействующих между собой с помощью средств связи.

Локальная вычислительная сеть (ЛВС) — это коммуникационная система, поддерживающая в пределах здания или группы зданий один или несколько высокоскоростных каналов передачи цифровой информации, подключенных к устройствам (ЭВМ) кратковременно. В настоящее время ЛВС применяются для объединения ЭВМ в различных масштабах: от рабочих групп, до сетей предприятия и кампусных сетей.

Маршрутизатор (узел маршрутизации), router — узел, управляющий пересылкой данных по сети с использованием системы адресов третьего сетевого уровня семиуровневой эталонной модели взаимодействия открытых систем (ЭМВОС).

Маска — это число, двоичная запись которого содержит единицы в разрядах, соответствующих номерам сети и подсети. Все единицы должны идти подряд, без пропусков. Маска используется совместно с IP-адресом.

Пакет или элемент данных протокола — передающийся по сети форматированный элемент данных, который включает в себя полезную и служебную информацию.

Префикс — число, показывающее количество единиц в маске.

Привратник — это специализированный сервер, который выполняет следующие функции:

- регистрация терминалов и других устройств;
- контроль доступа пользователей к услугам;
- преобразование телефонного номера или другой адресной информации в IP-адрес;
- контроль, управление и резервирование пропускной способности сети.

Протокол — набор правил для одной из коммутационных функций. Например, PPP (Point to Point Protocol) — протокол для организации канала передачи данных в режиме «точка-точка», а IP (Internet Protocol) — набор правил для маршрутизации данных.

Сеть доступа — набор технических и программных средств (мультиплексоры, модемы, линии связи, протоколы и др.), обеспечивающих абонентам выход в СПД.

Сетевой уровень — уровень межсетевого взаимодействия IP — Internet Protocol совпадает с сетевым уровнем ЭМВОС. Основное его назначение — выбор маршрута следования пакетов по определенному критерию и передача пакета по этому маршруту в составных сетях независимо от протоколов канального уровня.

Стек протоколов — набор организованных по уровням ЭМВОС протоколов, которые, работая совместно, позволяют прикладным процессам обмениваться данными. Например, стеком протоколов являются PPP, IP, TCP.

Структуризация сети — большие сети разбивают на отдельные однородные сегменты, между которыми помещаются активные устройства, регенерирующие сигнал с целью усиления и восстановления формы, а также ограничивающие взаимный трафик.

Сеть доступа — это совокупность абонентских и соединительных линий, узлов концентрации нагрузки и станций местной сети, обеспечивающих выход абонентов через свои терминалы в транспортную сеть или местную сеть без использования транспортной сети.

Сеть передачи данных — выделенная или наложенная система телекоммуникаций, которая через узлы маршрутизации (коммутации) и сеть доступа позволяет абонентам обмениваться различной информацией, представленной в цифровой

форме в виде последовательного набора фрагментов сообщения (пакетов). Другое определение сети является более узким и направлено только на вычислительные способности распределенных систем.

Узел коммутации или сетевой узел — элемент сети, где происходит перераспределение потоков данных по различным направлениям. При этом не конкретизируется, на базе каких протоколов и аппаратных средств (хаб, коммутатор, маршрутизатор и т. п.) это реализуется.

Хост — компьютер, который выполняет как приложения, так и сетевые функции и является конечной точкой сети. Как персональные компьютеры, так и мини-ЭВМ и большие ЭВМ попадают под определение хоста.

Шлюз — устройство, осуществляющее связь АС через пограничные маршрутизаторы.

Учебное издание

Пуговкин Алексей Викторович

СЕТИ ПЕРЕДАЧИ ДАННЫХ

Учебное пособие

Корректор Осипова Е. А.
Компьютерная верстка Перминова М. Ю.

Издано в Томском государственном университете
систем управления и радиоэлектроники.
634050, г. Томск, пр. Ленина, 40
Тел. (3822) 533018.