ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М. А. БОНЧ-БРУЕВИЧА»

А.В. Бородко, Д.С. Кукунин

КОМПЬЮТЕРНЫЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ
Часть 1

САНКТ-ПЕТЕРБУРГ
2013

УДК 681.326(075)
ББК З.8.8стд1-01.4

Рецензенты:
Н.В. Савищенко – доктор технических наук, профессор военной академии связи имени С.М. Буденного.
Е.М. Доронин – кандидат технических наук, доцент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Бородко А.В., Кукунин Д.С.
Учебное пособие по дисциплине КСПД. Часть 1 / ГОУВПО СПбГУТ. – СПб, 2013.
Излагаются теоретические основы по дисциплине компьютерные сети передачи данных. Рассмотрены физический, канальный и сетевой уровни протоколов организации локальных КСПД.
Предназначено для студентов, бакалавров специальности 210700, а также магистров и специалистов в области телекоммуникаций.

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ОСНОВНЫЕ КОНЦЕПЦИИ И ТЕРМИНЫ

1.1. Основные понятия и определения в области передачи дискретных сообщений

Информация - это совокупность сведений, являющихся объектом некоторых операций: передачи, распределения, преобразования, хранения или непосредственного использования. Для того, чтобы информацию можно было хранить и передавать, ее представляют в виде сообщений.

Сообщение - это форма представления информации для ее хранения, обработки, преобразования или непосредственного использования, т.е. совокупность знаков (символов), содержащих ту или иную информацию.

Сигнал - это физический процесс, отображающий передаваемое сообщение, т.е. форма представления информации для передачи её по каналу связи.

Сигнал всегда представляет собой функцию времени.

Канал связи или просто **канал** - заданная совокупность средств передачи информации, включающих в себя физическую среду.

Под каналом можно понимать любую часть системы связи, которую нельзя или нежелательно изменять.

Для сообщений, сигналов и каналов рекомендованы следующие обобщения. В зависимости от множества возможных сообщений (сигналов), а также области и характера их определения во времени, различают четыре вида сообщений и сигналов, и соответствующих им основных вида каналов (рис. 1.1): где графикам соответствуют следующие виды сигналов:

1.непрерывные непрерывного времени;
2.непрерывные дискретного времени;
3.дискретные непрерывного времени;
4.дискретные дискретного времени.

Для первого или второго и третьего или четвертого видов сообщений, сигналов и каналов приняты сокращенные названия *непрерывный* (аналоговый) и *дискретный* соответственно. Четвертый вид сигналов и каналов называют *цифровыми*.

Число возможных элементов сигнала на входе дискретного канала называют *основанием канала*. Например, двоичный канал, q-ичный канал.

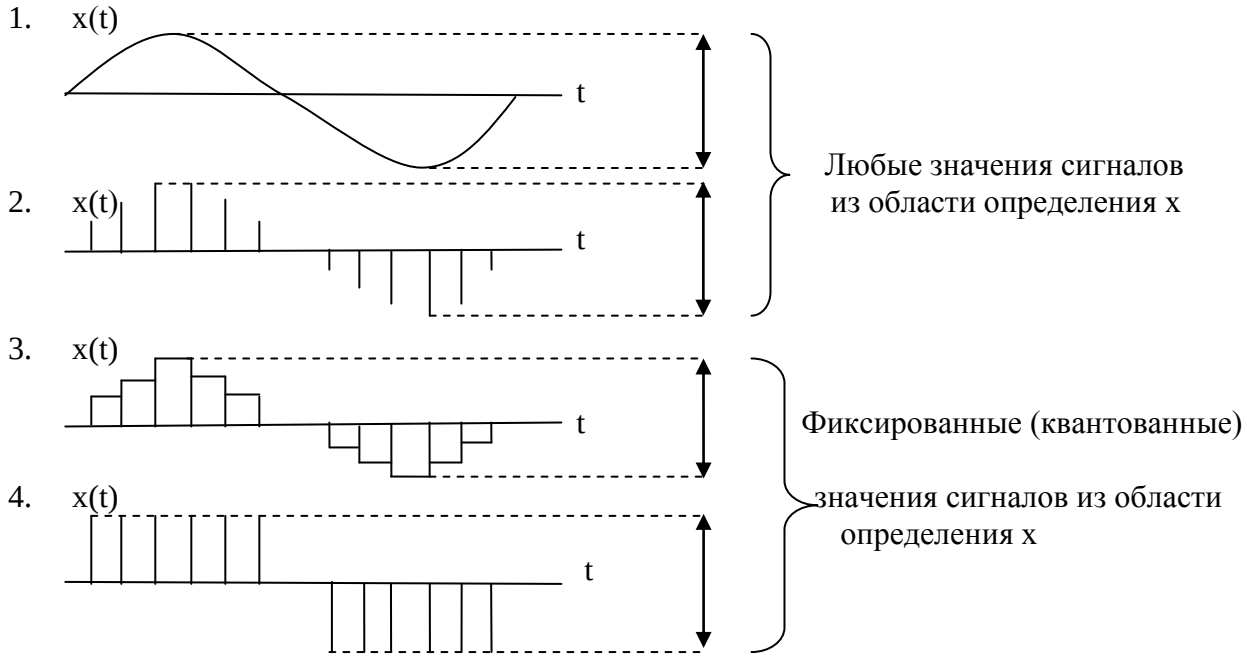


Рис.1.1

Модуляция - изменение во времени одного или нескольких параметров сигнала в соответствии с передаваемым сообщением. Параметры сигнала, которые отображают измерения передаваемого сообщения, называют *представляющими параметрами.*

Дискретные сигналы, состоящие из последовательностей импульсов постоянного тока, могут быть непосредственно (без дополнительных преобразований) переданы на то или иное расстояние только по некоторым видам каналов, обеспечивающих прохождение спектра этих сигналов. Для надёжной передачи дискретных сигналов применяется *модуляция*.

В двоичном канале передаются двоичные сигналы, условно обозначаемые цифрами «0» и «1». Их называют *двоичными единицами информации* или *битами*.

Введённые понятия и определения позволяют сформировать облик аппаратуры передачи дискретных сообщений и на этой основе продолжить ознакомление с компонентами системы передачи дискретных сообщений, являющимися составной частью компьютерных сетей передачи данных**.**

Физическое кодирование - способы представления двоичных данных в виде электрических или оптических импульсов. Кодирование сигнала на физическом уровне позволяет приемнику синхронизироваться с передатчиком по смене напряжения в середине периода битов, так как при кодировании бита 0 напряжением 0 вольт и бита 1 — напряжением +U вольт невозможно отличить «отсутствие сигнала» от бита 0. С точки зрения физического кодирования цифровой сигнал может иметь несколько уровней амплитуды напряжения.

Рассмотрим используемые в КСПД системы физического кодирования.

Метод **инверсного кодирования без возврата к нулю** (Non Return to Zero Invertive – NRZI). Данный способ является модифицированным методом без возврата к нулю (Non Return to Zero – NRZ), где для представления 1 и 0 используются два уровня напряжения. В коде NRZI тоже применяются два уровня напряжения, но его текущее значение зависит от предыдущего. Если текущее значение бита «1», то полученный потенциал должен быть инверсией от предыдущего, если значение бита «0», то значение повторяется (рис. 1.2).

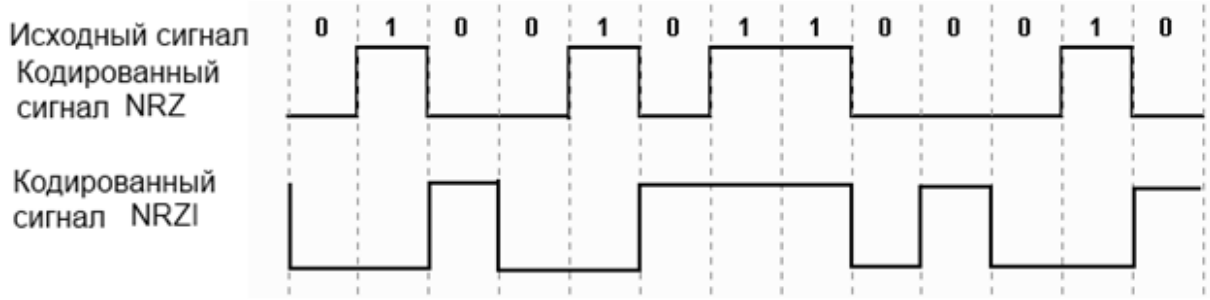


Рис. 1.2. Кодирование кодами NRZ и NRZI

Так как код изначально не защищен от долгих последовательностей «нулей» или «единиц», то передача длинных серий одинаковых символов может привести к проблемам синхронизации. Поэтому перед передачей, необходимую последовательность битов рекомендуется предварительно закодировать кодом, использующим скремблирование (скремблер предназначен для придания свойств случайности передаваемой последовательности данных путем применения логической операции суммирования по модулю 2 исходного и преобразующего псевдослучайного двоичных сигналов).

Код **Манчестер-II** или **манчестерский код** получил широкое распространение при построении локальных КСПД. Он также относится к самосинхронизирующимся кодам, но в отличие от кода NRZI имеет не три, а только два уровня, что обеспечивает лучшую помехозащищенность. Логическому нулю соответствует переход на верхний уровень в центре битового интервала, логической единице – переход на нижний уровень. Логика кодирования хорошо видна на примере передачи последовательности единиц или нулей. При передаче чередующихся битов частота следования импульсов увеличивается в два раза (рис. 1.3).

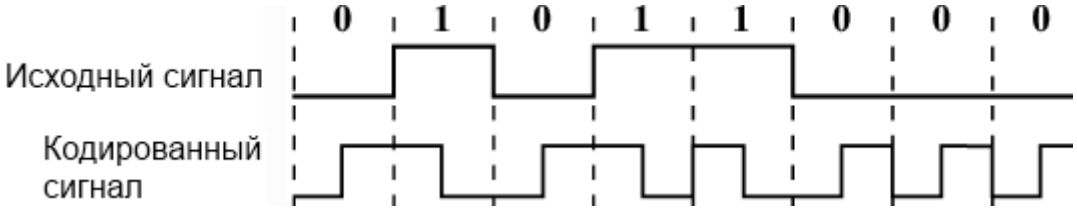


Рис. 1.3. Кодирование кодом Манчестер-II

Метод кодирования **MLT-3** (Multi Level Transmission) — похож на код NRZI, но в отличие от него оперирует тремя уровнями сигнала.

«Единица» кодируется переходом с одного уровня сигнала на другой, причем изменение уровня сигнала происходит последовательно с учетом предыдущего перехода. При передаче «нуля» передается нулевой уровень (рис. 1.4).

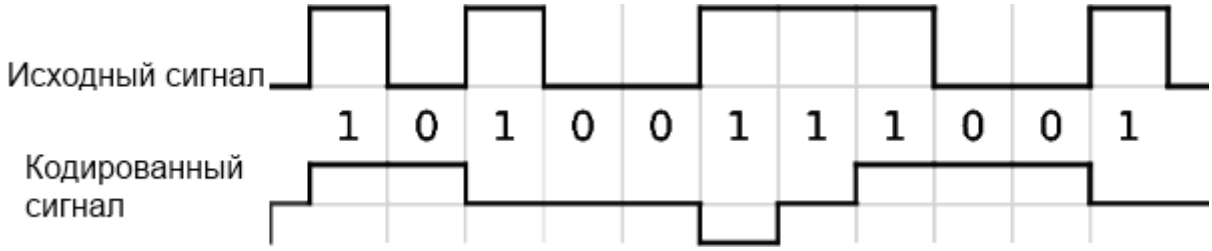


Рис. 1.4. Кодирование кодом MLT-3

PAM-5 (5-уровневое импульсно-амплитудное кодирование). В этом кодировании используется 5 уровней амплитуды и дополнительное двухбитное кодирование. Для каждой комбинации задается уровень напряжения. При двухбитовом кодировании для передачи информации необходимо четыре уровня (00, 01, 10, 11), как показано на рис. 1.5. Передача двух битов одновременно обеспечивает уменьшение в два раза частоты изменения сигнала (модуляции).

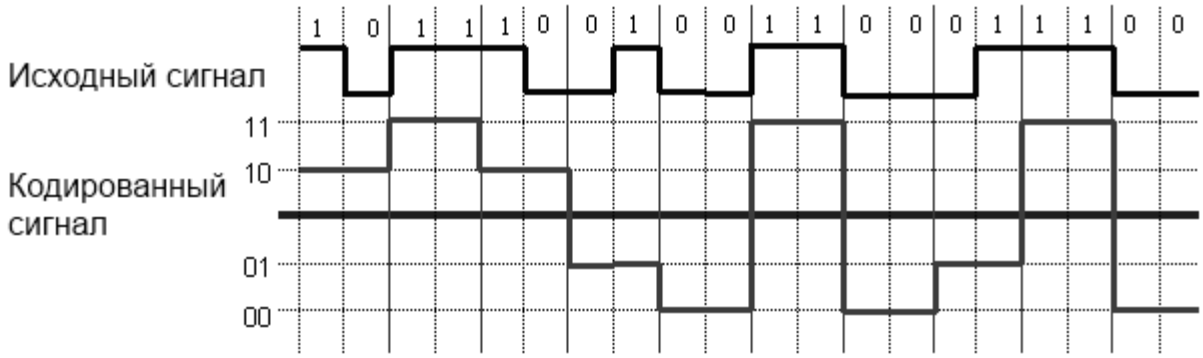


Рис. 1.5. Кодирование кодом PAM 5

Пятый уровень добавлен для создания избыточности кода, используемого для исправления ошибок, что может дать дополнительный прирост отношения сигнал-шум в 6 дБ.

Алгоритм 4B/5B выполняет преобразование 4 бит исходного сигнала в 5 бит выходного сигнала. Пятибитовая схема дает 32 (два в пятой степени) двухразрядных буквенно-цифровых символа, имеющих значение в десятичном коде от 00 до 31. Преобразованный сигнал имеет 16 значений для передачи информации и 16 избыточных значений. Избыточность кода, которую мы получили, позволяет использовать специальные комбинации для управления потоком и проверки подлинности принятой комбинации. Но использование такого кода увеличивает частоту передаваемого сигнала на 25%.

Алгоритм 8B/6T преобразовывает восьмибитовый октет данных в шестибитовый тринарный символ. Кодовые группы 6T предназначены для передачи параллельно по трем парам кабеля, в каждом из которых передается либо сигнал нулевого уровня, либо сигнал высокого или низкого уровней, поэтому эффективная скорость передачи данных по каждой паре составляет треть от исходной скорости передачи.

Например для передачи 100Base-T4 передача идет по трем парам кабеля, поэтому эффективная скорость передачи данных по каждой витой паре составляет треть от исходных 100 Мбит/с, следовательно, 33,33 Мбит/с. Скорость передачи тринарных символов по каждой паре составляет 6/8 от 33,3 Мбит/с, что соответствует тактовой частоте 25 МГц для передачи в каждой паре.

1.1.1. Основные параметры и характеристики системы ПДС

Основными характеристиками системы ПДС являются **достоверность**, **скорость** и **надежность** передачи дискретных сообщений.

Достоверность определяется следующими величинами:

1. Вероятностью ошибочного приема кодовых символов в результате неправильного решения регистрирующего устройства (РУ) при искажениях длительности единичных элементов; для этой вероятности принято обозначение $\boldsymbol{p}$, которое для существующих дискретных каналов – $p=10^{-4}\div10^{-2}$;
2. Вероятностью искажения кодовых комбинаций первичного кода, поступающих на вход канала передачи данных и выдаваемых получателю сообщений с ошибками в результате наличия ошибок в кодовых символах; для этой вероятности принято обозначение $p(\geq1,\ell)$, что означает наличие хотя бы одной ошибки в комбинации первичного кода длины $\boldsymbol{\ell}$. Для существующих каналов передачи
$$p(\geq1,\ell)\leq10^{-9}\div10^{-6}. \qquad (1.1)$$

Для определения скорости передачи дискретных сообщений существует два подхода.

Первый подход – *информационный*. Он требует умения измерять количество информации в сообщениях на выходе канала передачи данных относительно входных сообщений. При этом скорость передачи информации определяется как отнесенное к единице времени количество информации об ансамбле входных сообщений, содержащееся в выходных сообщениях.

Максимальную скорость передачи информации при заданных характеристиках канала, когда максимум берется по всем возможным вероятностным характеристикам сигнала, подаваемого на его вход, называют **пропускной способностью** канала или системы связи.

Второй подход – структурный. Он основан на подсчете структурных единиц сообщения, поступающих в приемник за некоторые временные интервалы.

Находят применение следующие характеристики скорости передачи дискретных сообщений:

- **скорость передачи единичных элементов** (R_e) – величина, обратная единичному интервалу, измеряемому в секундах.

Единицей измерения этой скорости является $\boldsymbol{c^{-1}}$;

- **скорость передачи битов данных** ($R_б$) – количество битов, переданных за единицу времени. Единицей измерения этой скорости является ***бит/с***. Определяется по формуле:

$$R_б = R_e \cdot log_2 m, \qquad (1.2)$$

где $\boldsymbol{m}$ – число значащих позиций на длине единичного элемента;

- **относительная скорость передачи данных** (R_o) – отношение числа битов данных, выданных получателю данных, к общему числу переданных битов;
- **эффективная скорость передачи данных** ($R_э$) – отношение числа битов данных, выданных получателю данных, к общему времени передачи, что соответствует:

$$R_э = R_o \cdot R_б. \qquad (1.3)$$

- Одной из наиболее часто используемых характеристик надежности передачи дискретных сообщений является **надежность своевременной доставки сообщений**, или **вероятностно-временная характеристика доведения(доставки) сообщения**. Она определяется следующим образом:

$$P(t_{дов} \le T_{зад}) \ge P_{доп}, \qquad (1.4)$$

что означает вероятность доведения (доставки) сообщения за время $\boldsymbol{t_{дов}}$, не превышающее некоторое заданное время $\boldsymbol{T_{зад}}$, должна быть не меньше допустимой вероятности $\boldsymbol{P_{доп}}$.

1.1.2. Упрощенная структурная схема аппаратуры ПДС

На рис. 1.6 представлена упрощённая структурная схема однозвенной аппаратуры передачи данных, являющейся типичным представителем аппаратуры передачи дискретных сообщений. Приведенные на рис. функциональные узлы аппаратуры соответствуют ГОСТ 17657-79, ГОСТ 34.936-91(ИСО 10039).

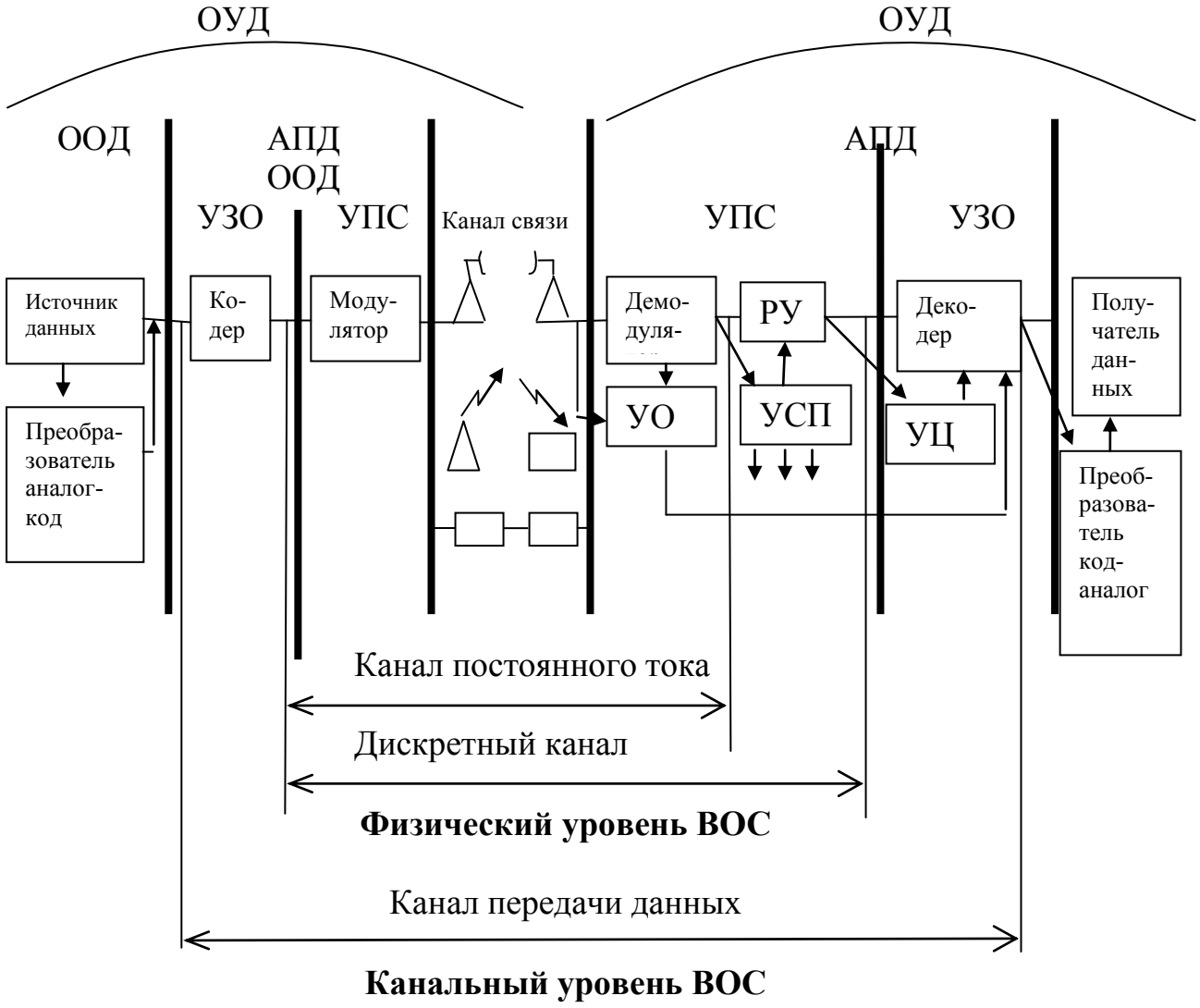


Рис.1.6. Упрощённая структурная схема однозвенной системы передачи данных

На рис. 1.6 приняты следующие обозначения:
ОУД – оконечная установка данных,
АПД – аппаратура передачи данных,
ООД – оконечное оборудование данных,
УЗО – устройство защиты от ошибок,
УПС – устройство преобразования сигналов,
РУ – регистрирующее устройство,
УОНС – устройство оценки надежности сигнала,
УСП – устройство синхронизации по элементам,
УЦС – устройство цикловой синхронизации.

Оконечное оборудование данных (ООД) представляет собой совокупность устройств ввода и вывода данных. Эти устройства на рис.1.2 представлены источником и получателем сообщений данных. Как правило, это технические средства. Источник формирует сообщение для его дальнейшей передачи, а приемник отображает сообщение в виде, адекватном его содержанию, для представления пользователю. Сообщения данных по своей природе имеют вид, о котором говорилось выше.

В случае аналоговых сообщений они подвергаются дополнительной обработке с помощью преобразователей «аналог – код» на передающей стороне и «код – аналог» - на приемной.

Обычно ввод сообщения от источника данных управляется со стороны АПД, а вывод к получателю – принудительный по мере поступления сообщений.

Аппаратура передачи данных (АПД) – совокупность средств, указанных на рис.1.2. К ним могут быть добавлены вспомогательные устройства, например, контрольно-измерительные устройства, устройства автоматического вызова и ответа и т.д.

Оконечная установка данных (ОУД) – совокупность оконечного оборудования данных и аппаратуры передачи данных, объединенных общим для них устройством управления (на рис. не представлено).

Устройство защиты от ошибок (УЗО) предназначено для уменьшения числа ошибок, появляющихся в сообщении данных под воздействием помех в канале связи. УЗО включает в свой состав устройства для помехоустойчивого кодирования и декодирования сообщений (кодер, декодер) и устройство цикловой синхронизации (УЦС). Кодер преобразует простой код, в котором сообщение поступает в АПД из ООД, в помехоустойчивый, а декодер выделяет из кодовых комбинаций помехоустойчивого кода, пришедших из канала связи, сообщение источника, устраняя при этом часть ошибок, появившихся при передаче сообщения по каналу связи в результате воздействия помех.

Устройство цикловой синхронизации (УЦС*)* устанавливает и поддерживает требуемые фазовые соотношения между циклами обработки передаваемых сообщений в кодере и декодере.

Устройство преобразования сигналов (УПС) предназначено для приведения сигнала сообщения, сформированного в ОУД, к виду, обеспечивающему ему передачу по каналу электросвязи. Основной состав УПС представлен на рис.1.2.

Модулятор – устройство, осуществляющее модуляцию. **Демодулятор** осуществляет обратное преобразование. Совокупность модулятора и демодулятора образует **модем.**

Регистрирующее устройство (РУ) осуществляет определение и запоминание значащей позиции принятого сигнала в пределах каждого еди-

ничного интервала, т.е. в двоичном случае определяет и запоминает значение каждого принятого бита.

Устройство оценки надежности сигнала (УОНС) – устройство, измеряющее один или несколько параметров принятого сигнала и вырабатывающее специальный сигнал, указывающий на возможные ошибки. Здесь и далее под *ошибкой* будем понимать событие, состоящее в том, что воспроизводимая приемником АПД последовательность сигналов не соответствует исходной. Ошибочный единичный элемент появляется на выходе РУ как результат неправильного решения РУ о значении принятого единичного элемента, ошибочная кодовая комбинация – на выходе декодера как результат неправильного решения декодера о соответствии принятой кодовой комбинации переданной. УОНС призван сократить число ошибок на выходе приемника АПД. Это достигается обработкой – стиранием единичного элемента на выходе РУ или отказом от декодирования – стиранием кодовой комбинации. Эти решения принимаются, в том числе, и на основе результатов работы УОНС.

Устройство синхронизации по элементам (или поэлементной синхронизации) (УСП) обеспечивает синхронизацию переданного и принятого сигналов, при которой устанавливаются и поддерживаются требуемые фазовые соотношения между значащими моментами переданных и принятых единичных элементов этих сигналов.

Кратко опишем процесс передачи информации в рассматриваемой системе.

Источник вырабатывает сообщение. Если это сообщение имеет дискретную природу (буквы, цифры и т.п.), то оно на выходе источника представляется в виде комбинаций простого кода. Обычно для этой цели используются пятиэлементные коды или семиэлементные коды, называемые первичными. Если вырабатываемое сообщение является аналоговым (изменение температуры, уровня радиации, освещенности и т.п.), то с помощью цифро-аналогового преобразователя («аналог – код») оно приводится к дискретной форме и затем представляется в виде последовательности комбинаций первичного кода.

По команде от АПД сообщения от источника данных вводятся в *кодер*. Здесь ℓ-элементная комбинация первичного кода преобразуется в n-элементную комбинацию избыточного кода, где $n > \ell$. В комбинации избыточного кода помимо элементов, несущих информацию источника сообщений (информационные элементы), вводятся по определенному правилу избыточные элементы, обеспечивающие коду помехоустойчивые свойства. Далее побитно n-элементная комбинация вводится в виде сигналов постоянного тока в *модулятор*, где сигналы постоянного тока преобразуются к виду, согласованному с используемым каналом, и с помощью каналообразующей аппаратуры через среду распространения поступают на вход *демодулятора*, где осуществляется обратное преобразование модулированного

сигнала в сигналы постоянного тока. При прохождении электрического сигнала по каналу связи на него воздействуют различного рода помехи, которые проявляются в виде искажений длительности сигналов постоянного тока на выходе *демодулятора*.

УСП определяет ожидаемые значащие моменты поступающих на вход РУ импульсов постоянного тока, и РУ восстанавливает значащие позиции принятых сигналов на значащих интервалах.

С выхода РУ принятое сообщение побитно поступает в *декодер*. С помощью УЦС определяется начало принятых n-элементных комбинаций. Декодер на основе связей между информационными и избыточными элементами выделяет информационные элементы, и УЗО принудительно выводит их к получателю данных в виде ℓ-элементных комбинаций. Принятые сообщения в зависимости от их первоначальной формы выдаются получателю либо в дискретной форме (комбинации первичного кода), либо с помощью *цифро-аналогового преобразователя* («код – аналог») в непрерывной форме.

Для обеспечения целевого назначения рассматриваемой системы к ней предъявляются определенные требования.

Так как система связи является сложной системой, то для предъявления требований к ней она декомпозируется на составные части.

На рис.1.6 в рассматриваемой системе связи выделяются три составные части:

- канал постоянного тока,
- дискретный канал,
- канал передачи данных.

Канал постоянного тока, как это видно из рис. 1.6, представляет собой часть системы связи от входа модулятора до выхода демодулятора. Сигналы на входе и выходе этого канала являются импульсами постоянного тока, к которым предъявляются требования по величине искажений, т.е. канал постоянного тока нормируется по величине искажений длительности передаваемых и принимаемых сигналов.

Дискретный канал – часть системы связи от выхода кодера до входа декодера. На входе и выходе этого канала сигналы имеют вид последовательностей кодовых символов; в двоичном случае – последовательностей двоичных единиц. Выход этого канала – выход РУ, который характеризуется возможностью появления ошибок в результате превышения допустимой величины искажения длительности сигналов на входе РУ. Дискретный канал вводится для задания требований, т.е. нормирования вероятности появления ошибок в кодовой последовательности на входе декодера УЗО.

Канал передачи данных - часть системы связи от входа кодера до выхода декодера. На входе и выходе этого канала передаваемые сообщения имеют вид кодовых комбинаций первичного кода. Этот канал служит для задания требований, т.е. нормирования потока комбинаций первичного ко-

да по вероятности искажения кодовой комбинации первичного кода. Реализация этих требований позволяет снизить вероятность ошибки в комбинации первичного кода, поступающей к получателю, до заданной величины. Поэтому канал передачи данных называют защищенным от ошибок каналом.

1.2. Переход от упрощенной структурной схемы системы ПДС к компьютерным сетям ПД

Коммуникационная сеть — система, состоящая из объектов, осуществляющих функции генерации, преобразования, хранения и потребления продукта, называемых пунктами (узлами) сети, и линий передачи (связей, коммуникаций, соединений), осуществляющих передачу продукта между пунктами.

Отличительная особенность коммуникационной сети — большие расстояния между пунктами по сравнению с геометрическими размерами участков пространства, занимаемых пунктами. В качестве продукта могут фигурировать информация, энергия, масса, и соответственно различают группы сетей информационных, энергетических, вещественных. В группах сетей возможно разделение на подгруппы. Так, среди вещественных сетей могут быть выделены сети транспортные, водопроводные, производственные и др. При функциональном проектировании сетей решаются задачи синтеза топологии, распределения продукта по узлам сети, а при конструкторском проектировании выполняются размещение пунктов в пространстве и проведение (трассировка) соединений.

Информационная сеть — коммуникационная сеть, в которой продуктом генерирования, переработки, хранения и использования является информация.

Вычислительная (компьютерная) сеть — информационная сеть, в состав которой входит вычислительное оборудование. Компонентами вычислительной сети могут быть ЭВМ и периферийные устройства, являющиеся источниками и приемниками данных, передаваемых по сети. Эти компоненты составляют оконечное оборудование данных (ООД или DTE — Data Terminal Equipment). В качестве ООД могут выступать ЭВМ, принтеры, плоттеры и другое вычислительное, измерительное и исполнительное оборудование автоматических и автоматизированных систем. Собственно пересылка данных происходит с помощью сред и средств, объединяемых под названием ***среда передачи данных***.

1.2.1. Основные характеристики КСПД

Аналогично тому, как основными характеристиками системы передачи дискретных сообщений являются достоверность, скорость и надежность передачи (см. раздел 1.1.1.), а дискретный канал характеризуется скоростью модуляции, скоростью передачи информации, пропускной способностью, достоверностью и надежностью, подобные характеристики можно применить и к сети ПД:

Пропускная способность сети – максимальный объем информации, поступающей на входы сети в некоторый интервал времени и обслуживаемый сетью с заданными показателями качества.

Производительность сети – среднее количество информации, поступающее на входы сети в некоторый интервал времени и обслуживаемый сетью с заданными показателями качества; производительность сети – реализуемая пропускная способность сети.

Пиковая производительность сети – максимальный объем информации, поступающей на входы сети в ограниченный интервал времени и обрабатываемый сетью с заданными показателями качества.

Нагрузка сети. Под нагрузкой (трафиком) сети понимают количество сообщений, передаваемых или обрабатываемых в сети в единицу времени. Аналогичным образом определяется нагрузка для любого элемента сети.

Вероятность своевременного доведения сообщения – вероятность того, что сообщение заданного объема будет доставлено адресату за время, не превышающее допустимое:

$$P(T_{дов} \le T_{доп}) \ge P_{зад} \qquad (1.6)$$

Эта вероятность получила название вероятностно-временной характеристики сети.

Надежность сети – способность сети функционировать заданным образом в нормальных условиях эксплуатации.

Живучесть сети – способность сети обеспечивать передачу сообщений при выходе из строя ее элементов.

Безопасность сети – способность сети обеспечивать целостность передаваемых сообщений и их конфиденциальность.

1.3. Эталонная модель взаимодействия открытых систем (ЭМ ВОС)

Для согласования работы устройств сети от разных производителей, обеспечения взаимодействия сетей, которые используют различную среду распространения сигнала и имеют различную архитектуру создана эталонная модель ВОС (модель open systems interconnection – OSI) (ГОСТ Р

ИСО/МЭК 7498-1-99). Этот стандарт подготовлен методом прямого применения стандартов МОС 7498-84, МОС 7498-84 Доп. 1 и полностью им соответствует. Аналогичные рекомендации содержатся в восьмом томе Синей книги МККТТ, ныне секции стандартизации Международного Союза электросвязи (МСЭ), - рекомендация Х.200.

Основу ЭМВОС составляют четыре элемента: открытые системы, прикладные процессы и соответствующие им прикладные логические объекты, существующие в рамках ВОС, соединения, которые связывают прикладные логические объекты и позволяют им обмениваться информацией, и физическая среда для ВОС.

Прежде чем приступить к определению основных принципов построения модели важно определиться понятиями, используемыми в стандартах ВОС, как, реальная система, реальная открытая система, открытая система, прикладной процесс, прикладной логический объект и соединение.

Реальная система (РС) – это совокупность одной или нескольких ЭВМ, программного обеспечения, терминалов и других средств, а также операторов, которая образует полностью автономную систему, спо-собную обрабатывать и передавать информацию.

Реальная открытая система (РОС) – это реальная система, которая подчиняется требованиям стандартов ВОС при взаимодействии с другими системами.

Открытая система (ОС) – представление в рамках эталонной модели тех аспектов реальной открытой системы, которые относятся к ВОС.

Прикладной процесс (ПП) – элемент реальной открытой системы, который выполняет обработку информации для некоторого конкретного применения. Это может быть ручной процесс, процесс, выполняемый на ЭВМ, или физический процесс.

Физическая среда для связи ОС предназначена для передачи информации между ними. В качестве физической среды обычно выступают каналы связи различной физической природы.

Структура эталонной модели показана на рис. 1.7.

Эталонная модель состоит из семи уровней. Нумерация уровней начинается с нижнего и заканчивается верхним. Все уровни делятся на две группы. Верхние три уровня ориентированы на программное обеспечение. Их работа не зависит от работы сети. Нижние уровни являются сетезависимыми, т. е. они зависят от сети, но не зависят от программных уровней.

Эталонная модель построена по иерархическому принципу. Каждый уровень обеспечивает сервис вышестоящему уровню и пользуется услугами нижестоящего уровня.

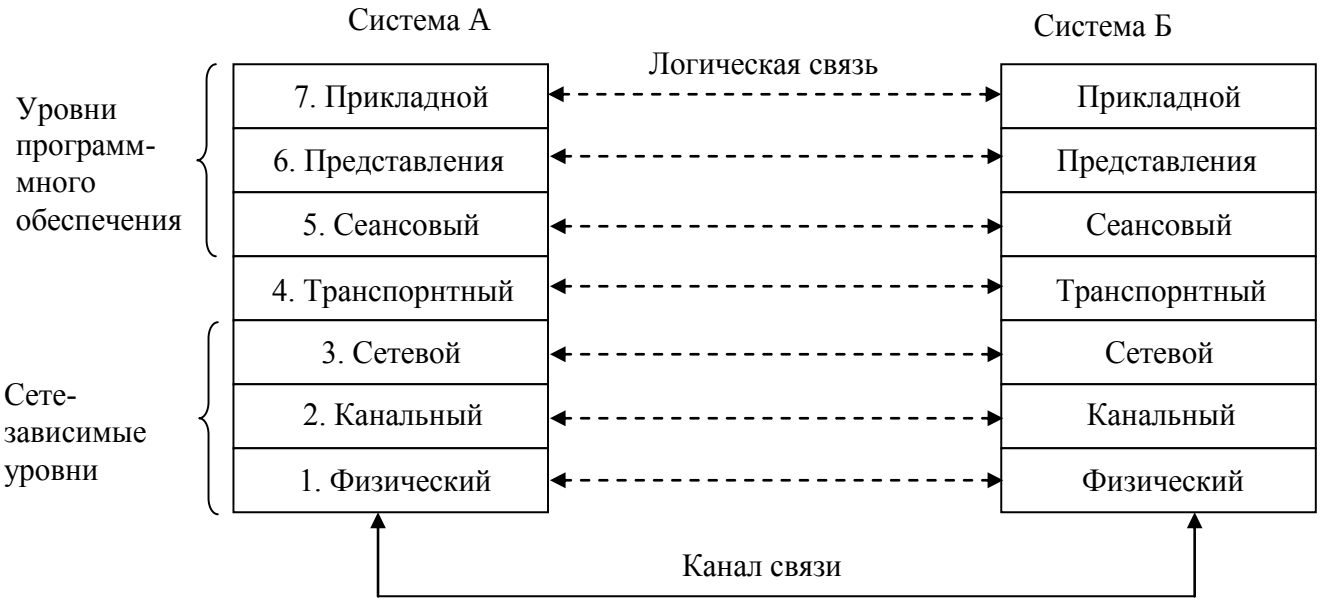


Рис. 1.7. Структура эталонной модели ВОС

Обработка сообщений начинается с прикладного уровня. После этого, данные проходят через все уровни эталонной модели, и через физический уровень отправляются в канал связи. На приеме происходит обратная обработка данных. Каждый уровень работает по определенным правилам, на основе которых к данным на каждом уровне прикрепляется заголовок со служебными данными, при этом процедуры взаимодействия элементов одного уровня называют протоколами.

Протокол – это набор правил, на основе которых взаимодействуют одноименные уровни различных систем.

Заголовок, который формируется на каждом уровне, предназначен только для протокола одноименного уровня смежной системы. Другие уровни прочитать этот заголовок не могут. Поэтому считается, что между одноименными уровнями смежных систем существует логическая связь.

1.3.1. Назначение уровней

В соответствии с моделью ВОС каждый уровень может быть описан совокупностью выполняемых им функций. Эти функции, в общем случае, включают в себя:

- выбор протокола;
- установление и разрыв соединения;
- мультиплексирование и расщепление соединений;
- передачу обычных и срочных данных;
- управление потоком данных;
- сегментирование блокирование и сцепление данных;

- организацию последовательности;
- защиту от ошибок;
- маршрутизацию.

Прикладной уровень. Обеспечивает интерфейс пользователя КСПД с сетевыми службами и к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организацию совместной работы, например, с помощью протокола электронной почты. На прикладном уровне осуществляются прикладные процессы, т. е. ввод данных, редактирование, удаление. К сетевым службам относятся: электронная почта, телеконференция, доска объявлений и т.д.

Протоколы этого уровня отвечают за идентификацию и установление доступности предполагаемого партнера по диалогу. Здесь же определяется, достаточно ли ресурсов для взаимодействия.

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

Уровень представления. Этот уровень отвечает за то, как будут представлены данные пользователю. На этом уровне осуществляется кодирование и декодирование данных, сжатие и распаковка, соответствие текста стандартизованным кодовым таблицам. Здесь данные форматируются, или, как иногда говорят, транслируются для представления их на уровне приложений. Для удобства передачи данные перед пересылкой приводятся к стандартному формату. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Согласно протоколам этого уровня принятые данные преобразуются в формат, пригодный для чтения (например, транслируются из кода EBCDIC в код ASCII).

Уровень представления обеспечивает для прикладного уровня следующие функции:
- соглашение по выбору и повторному выбору синтаксиса;
- преобразование синтаксиса, включая преобразование данных, формирование и специальные функции преобразования (например, сжатие);
- запрос на завершение сеанса.

Сеансовый уровень. Этот уровень обеспечивает диалог, т.е. взаимодействие рабочих станций в течение всего сеанса связи. Таким образом, он отвечает за поддержание сеанса связи, т.е. за его начало и завершение. Взаимодействие ОС, организуемое на этом уровне, может происходить в трех различных режимах: симплексном, полнодуплексном и полудуплексном, с выбором активной стороны, а также может предоставлять средства синхронизации. Сеансовый уровень обычно занимается отделением данных одного приложения от информации другого приложения. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Транспортный уровень. Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети, т.е. компонентами их сетевых операционных систем, поэтому считается, что на этом уровне обеспечивается согласование верхних уровней, ориентированных на программное обеспечение и нижних, сетезависимых.

Основная функция протоколов этого уровня – доставка сообщений по сети от РОС источника до РОС получателя, с реализацией требований по своевременности и целостности. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции, например, функции передачи данных без подтверждения приема, и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, которые мультиплексируют несколько потоков данных, обеспечивая механизм управления потоками данных и гарантируют достоверность принятых данных путем использования помехоустойчивого кодирования с организацией канала обратной связи.

Передача данных может осуществляться в двух режимах:

- при *виртуальной коммутации пакетов* до передачи сообщения устанавливается логическое соединение между взаимодействующими объектами транспортного уровня (а возможно и более высоких уровней ОС). Этот логический канал запоминается в маршрутных таблицах всех узлов коммутации пакетов, которые участвуют в соединении. Пакеты передаются только по установленному логическому каналу, поэтому порядок их следования при этом не нарушается, однако, для реализации требуется наличие протоколов сетевого уровня с установкой соединения.
- при *дейтаграммной коммутации пакетов* логического соединения не устанавливается, поэтому пакеты одного сообщения передаются по тем маршрутам, которые оптимальны в данный момент, т.е. возможно разными маршрутами. Проблема сборки сообщения решается протоколами на транспортном уровне.

Единица контролируемой информации – *сегмент*. Согласно протоколам этого уровня происходит разбиение данных на сегменты, их циклическая нумерация и последующая сборка в сообщение.

Функции протоколов транспортного уровня:

- управление потоком данных;
- сегментирование, блокирование и сцепление данных;
- организацию последовательной нумерации сегментов;
- защиту от ошибок.

Сетевой уровень отвечает за маршрутизацию (т.е. для определения пути передачи данных) в КСПД и, соответственно, сетевую адресацию, т.е. за пересылку информации между РОС. Отвечает за адресацию РОС, транс-

ляцию логических адресов и имён в физические, определение кратчайших маршрутов, маршрутизацию, отслеживание неполадок в сети.

Протоколы сетевого уровня делятся на протоколы:

- *с установкой соединения,* которые начинают передачу данных с вызова или установки маршрута следования пакетов от источника к получателю, после чего начинают последовательную передачу данных и затем по окончании передачи разрывают связь;
- *без установки соединения*, которые посылают данные, содержащие полную адресную информацию в каждом пакете. Каждый пакет содержит адрес отправителя и получателя. Далее каждое промежуточное сетевое устройство считывает адресную информацию и принимает решение о маршрутизации данных. Письмо или пакет данных передается от одного промежуточного устройства к другому до тех пор, пока не будет доставлено получателю. Протоколы без установки соединения не гарантируют поступление информации получателю в том порядке, в котором она была отправлена, т.к. разные пакеты могут пройти разными маршрутами. За восстановления порядка данных при использовании сетевых протоколов без установки соединения отвечают протоколы транспортного уровня.

Единица данных, которой оперирует сетевой уровень, называется пакетом.

Функции протоколов сетевого уровня включают в себя:

- установление и разрыв соединения;
- мультиплексирование и расщепление соединений;
- передачу обычных и срочных данных;
- управление потоком данных;
- маршрутизацию.

Канальный уровень (уровень звена данных). Канальный уровень обеспечивает функциональные и процедурные средства для установления, поддержания и разрыва соединений уровня звена данных между сетевыми логическими объектами, а также средства для передачи сервисных блоков данных этого уровня. Протоколы уровня звена данных обнаруживают и по возможности исправляют ошибки, возникающие на физическом уровне и при передаче блоков данных через физическую среду.

Единица данных, которой оперирует уровень звена данных, называется кадром (frame).

Функции протоколов уровня звена данных включают в себя:

- упорядочение блоков данных;
- обнаружение ошибок;
- восстановление при ошибках;
- установление и разрыв соединения уровня звена данных;
- отображение сервисных блоков данных (кадров) уровня звена данных;
- управление потоком данных;
- идентификация и обмен параметрами;

- административное управление уровнем звена данных.

Физический уровень обеспечивает механические, электрические, функциональные и процедурные средства для активизации, поддержки и деактивизации физических соединений, предназначенных для побитовой передачи между логическими объектами уровня звена данных. Единица измерения, используемая на этом слое — Биты. Физический уровень взаимодействует с разными типами физических сред, что приводит к различному представлению битовых значений. Значения могут быть представлены тональными или фазовыми сигналами, но чаще битовые значения представлены переходами между состояниями — изменениями напряжения от низкого к высокому потенциалу или наоборот.

На физическом уровне определен интерфейс между оконечным оборудованием данных (DTE – Data Terminal Equipment) и аппаратурой окончания канала данных (DCE – Data Circuit-terminating Equipment). Если оконечное оборудование цепей передачи данных размещается у провайдера, то оконечным оборудованием данных являются подключенные устройства пользователей (РОС). Оконечное оборудование данных – это устройство, генерирующее или принимающее данные, а аппаратура окончания канала данных (в отечественной литературе встречается аналогичный термин АПД - аппаратура передачи данных) - это устройство, осуществляющее интерфейс между оконечным оборудованием данных и физической средой.

Реализация услуг физического уровня обеспечивается выполнением следующих функций:
- активизация и деактивизация физического соединения;
- передача физических сервисных блоков данных.

1.3.2. Разработчики стандартов

Международная организация по стандартизации (International Standards Organization – ISO) – основана в 1946 г. для разработки международных стандартов в различных областях техники, производственной и других видах деятельности. Объединяет более 70 национальных организаций по стандартизации. Наиболее известный стандарт ISO в области телекоммуникаций регламентирует семиуровневую модель взаимодействия открытых систем.

Американский национальный институт стандартов (American National Standards Institute)

Объединение американских промышленных и деловых групп, разрабатывающее торговые и коммуникационные стандарты. Входит в ISO, представляя там Соединенные Штаты Америки.

В сферу деятельности института стандартов входят коды, алфавиты, сигнальные схемы, языки программирования. Из принятых институтом стандартов наиболее известен ANSI X3.4 — 7-битная кодировка ASCII.

Основные стандарты и спецификации принятые институтом: интерфейс Token Ring, CSMA/CD, SQL, алгоритмы шифрования.

Международный союз электросвязи – **МСЭ** (International Telecommunication Union, ITU), ранее называвшийся Международный консультативный комитет по телефонии и телеграфии МККТТ (франц. Comite Consultatif Internationale de Telegraphie et Telephonie – CCITT)

Протоколы ITU-T относятся к модемам, сетям, передаче факсимильных сообщений.

В него входят 15 исследовательских групп: A и B – рабочие процедуры, термины и определения, I – ISDN, K и L – защита оборудования, R-U – терминальные и телеграфные услуги, V – передача данных по телефонным сетям, X – сети передачи данных.

Группа стандартов ITU-T на средства и методы обработки и передачи данных на физическом и канальном уровнях:

- **V.17** – стандарт **ITU-T** передачи данных со скоростью до 14,4 Кбит/с (используется для обмена факсимильными сообщениями).
- **V.21** – стандарт **ITU-T** для дуплексной передачи с частотным разделением каналов и частотной модуляцией. Скорость передачи 300 бит/с.
- **V.22** – стандарт **ITU-T** для дуплексной передачи с частотным разделением каналов со скоростью 600 бит/с или 1,2 Кбит/с по коммутируемому или выделенному каналу с применением двукратной относительной фазовой (фазоразностной) модуляции.
- **V.22bis** – стандарт **ITU-T** для дуплексной передачи с частотным разделением по коммутируемому каналу со скоростью 1,2 или 2,4 Кбит/с с применением амплитудной квадратурной модуляции.
- **V.23** – стандарт **ITU-T** для полудуплексной передачи со скоростью 1,2 Кбит/с по коммутируемому каналу с применением частотной модуляции.
- **V.24** – стандарт **ITU-T**, определяющий электрический **интерфейс** между терминальным оборудованием (**ООД**) и модемом. Эквивалентен интерфейсу **RS232C**, разработанному ассоциацией **EIA.**
- **V.26** – стандарт **ITU-T** для полудуплексной передачи со скоростью 2,4 Кбит/с по выделенному каналу с применением двукратной относительной фазовой модуляции.
- **V.26bis** – стандарт **ITU-T** для дуплексной передачи со скоростью 2,4 Кбит/с по коммутируемому каналу с применением двукратной относительной фазовой модуляции.
- **V.27** – стандарт **ITU-T** для дуплексной передачи со скоростью 2,4 Кбит/с по выделенному каналу с применением трехкратной относительной фазовой модуляции.
- **V.27ter** – стандарт **ITU-T** для полудуплексной передачи со скоростью 4,8 Кбит/с по коммутируемому каналу с применением трехкратной относительной фазовой модуляции.
- **V.29** – стандарт **ITU-T** для дуплексной передачи со скоростью 9,6 Кбит/с по четырех проводному выделенному каналу, а также для полудуплексной

передачи по коммутируемому или двухпроводному выделенному каналу с применением 16-позиционной квадратурной амплитудной модуляции. Широко используется также для передачи факсимильных сообщений со скоростью 9,6 Кбит/с и 7,2 Кбит/с.

- **V.32** – стандарт **ITU-T** для дуплексной передачи со скоростями 2,4; 4,8 или 9,6 Кбит/с по коммутируемому или двухпроводному выделенному каналу с применением 16-позиционной амплитудно-фазовой модуляции. Поддерживает методы исправления ошибок (решетчатое кодирование) и подавления помех за счет отраженного сигнала (эхо-компенсации).
- **V.32bis** – стандарт **ITU-T** для дуплексной передачи со скоростью 7,2; 9,6; 12,0 или 14,4 Кбит/с по коммутируемому или двухпроводному выделенному каналу с применением 128-позиционной квадратурной амплитудной модуляции. Поддерживает методы согласования скорости приема – передачи, исправления ошибок (решетчатое кодирование) и подавления помех за счет отраженного сигнала (эхо-компенсации).
- **V.32terbo** – спецификация фирмы **AT&T** , совместимая со стандартами V.32 и V.32bis. Описывает метод дуплексной передачи со скоростью 19,2 Кбит/с по коммутируемому или двухпроводному выделенному каналам.
- **V.33** – стандарт **ITU-T** для дуплексной передачи со скоростью 14,4 Кбит/с по четырех проводному выделенному каналу с применением 128-позиционной амплитудно-фазовой модуляции.
- **V.34** – стандарт **ITU-T** для дуплексной передачи со скоростью 33,6 Кбит/с по коммутируемому каналу.
- **V.35** – стандарт **ITU-T** , определяющий **интерфейс** между терминальным оборудованием (ООД) и **линейным драйвером** – преобразователем цифровых сигналов, улучшающим их характеристики для обеспечения надежности передачи на большие расстояния. Поддерживает скорость передачи до 64 Кбит/с.
- **V.42** – стандарт **ITU-T** для дуплексных модемов, описывающий методы исправления ошибок. Поддерживает **протокол доступа к каналу для модемов** (Link Access Protocol for Modems), совместимый с протоколами **LAPB** для сетей **X.25** и **LAPD** для сетей **ISDN**.
- **V.42bis** – стандарт **ITU-T**, описывающий процедуры сжатия данных, передаваемых модемами. Позволяет вчетверо увеличить скорость передачи данных, если принимающий модем также поддерживает этот стандарт.
- **V.70** – стандарт **ITU-T**, определяющий протокол одновременной передачи голоса и данных (DSVD).
- **V.90** – стандарт **ITU-T**, определяющий протокол для модемов и оборудования, рассчитанных на скорость передачи данных 56,7 Кбит/с (прямая передача) и 33,6 Кбит/с (обратная передача). Данный протокол принят в начале 1998 г. Он снимает возникшие ранее проблемы появления двух альтернативных стандартов: X2 фирмы Robotics (США) и K56Flex (альянс фирм – Lucent Technologues, Rokwell и др.).

- **V.92** – стандарт **ITU-T**, определяющий протокол для модемов и оборудования, рассчитанных на скорость передачи данных 56,7 Кбит/с. Это достигается за счет использования для кодирования данных с помощью импульсно – кодовой модуляции.
- **V.120** – стандарт **ITU-T**, определяющий протокол, который обеспечивает взаимодействие устройств, имеющих скорость передачи менее 64 Кбит/с. Ряд коммуникационных программных продуктов для ПЭВМ требуют, чтобы указанные устройства поддерживали протокол V.120.

Группа стандартов ITU-T на протоколы и интерфейсы, предназначенные для передачи цифровых данных:

- **X.21** – рекомендация **ITU-T**, описывающая физический **интерфейс** между терминалом и аппаратурой передачи данных. Предназначен для замены более ранних рекомендаций **V.24** и **V.25**.
- **X.25** – стандарт **ITU-T**, определяющий **интерфейс** между оконечным оборудованием (ООД) и аппаратурой передачи данных (АПД) для рабочих станций, действующих в режиме коммутации пакетов в сети передачи данных общего пользования. Реализует три уровня протокола: физический, канальный и сетевой. Термин X.25часто используется для обозначения сетей с коммутацией пакетов, что не совсем верно. Рекомендация X.25 специфицирует лишь интерфейс доступа к сети, но не устанавливает порядок функционирования сети и правила управления ею.
- **X.75** – стандарт **ITU-T** для сетей пакетной коммутации, описывающий структуру сообщений для обмена по международным каналам между шлюзами сетей **X.25.**
- **X.121** – стандарт **ITU-T**, определяющий международную систему адресации в **сетях X.25**.
- **X.400** – международный стандарт для систем передачи сообщений, описывающий методы электронного обмена (текстами, графикой, факсами и др.). Основное назначение стандарта – обеспечение взаимодействия между различными системами электронной почты. Определяет несколько протоколов, обеспечивающих надежную передачу между агентами пользователя и агентами передачи сообщений.
- **X.500** – стандарт **ITU-T** был принят в 1988 г., обновлялся в 1993 и 1997 гг. Предназначен для поддержки глобальной службы каталогов Интернет. Ядро X.500 составляет распределенная иерархическая справочная база данных обо всех поименованных объектах сети.

Общество Интернет (Internet Society, ISOC) – профессиональное сообщество, которое занимается общими вопросами эволюции и роста Интернет как глобальной коммуникационной инфраструктуры. Организация насчитывает более 20 тысяч индивидуальных членов и более 100 организаций-членов в 180 странах мира. Под управлением Общество Интернет работает **– Совет по архитектуре Интернет** (Internet Architecture Board, IAB) **–** группа технических советников, в ведении которой находится технический надзор за архитектурой Интернет и координация работ по созданию новых стандартов для

Интернет. IAB координирует направление исследований и новых разработок для стека TCP/IP и является конечной инстанцией при определении новых стандартов Интернет, а также редактирование и публикацию серии документов RFC.

В совет по архитектуре Интернет входят две основные группы:

1. **Инженерная целевая группа Интернет** (Internet Engineering Task Force, IETF) – международная общественная организация сообщества Интернет, которая отвечает за организацию работы системы, разработку стандартов сети и техническое усовершенствование средств ее обеспечения. Именно IETF определяет спецификации, которые затем становятся стандартами Интернет. Документ RFC 2031 описывает отношения ISOC и IETF.
2. **Исследовательская группа Интернет-технологий** (Internet Research Task Force, IRTF). Координирует долгосрочные исследовательские программы, связанные с вопросами развития архитектуры и базовых протоколов TCP/IP.

В настоящее время первичной публикацией документов под названием **рабочее предложение** (Request for Comments, RFC) занимается Инженерная целевая группа Интернет под эгидой открытой организации Общество Интернет. Правами на RFC обладает именно Общество Интернет. Список утвержденных официальных стандартов Интернет публикуется в виде документа RFC (Request for Comments) и доступен в Интернет. Все стандарты Интернет носят название RFC с соответствующим порядковым номером, но не все RFC являются стандартами.

Формат RFC появился в 1969 году при обсуждении проекта ARPANET. Первый документ был опубликован 7 апреля 1969 г. и назывался «Программное обеспечение узла» (Host Software). Первые RFC распространялись в печатном виде на бумаге в виде обычных писем, но уже с декабря 1969 г., когда заработали первые сегменты ARPANET, документы начали распространяться в электронном виде. Большинство ранних RFC были созданы в Калифорнийском университете Лос-Анджелеса и Стэнфордском исследовательском институте.

Примеры наиболее употребительных документов RFC:

RFC 768 – описывает протокол UDP,
RFC 791 – описывает протокол IP,
RFC 792 – описывает протокол ICMP,
RFC 793 – описывает протокол TCP,
RFC 821 – описывает протокол SMTP, впоследствии заменён RFC 2821,
RFC 822 – описывает формат электронной почты, заменён RFC 2822,
RFC 826 – описывает протокол разрешения адреса (ARP),
RFC 894 – описывает способ передачи IP пакетов по сетям Ethernet,
RFC 1034 – описывает концепцию DNS,
RFC 1518 – описывает присвоение адресов согласно бесклассовой адресации (CIDR),
RFC 1905 – описывает протокол SNMP,
RFC 1907 – описывает протокол SNMP версии 2,
RFC 2131 – описывает протокол DHCP,

RFC 2328 – описывает протокол OSPF,
RFC 2401 – описывает архитектуру безопасности протокола IP (IPsec),
RFC 2453 – описывает протокол RIP,
RFC 2616 – описывает протокол HTTP.

Ассоциация электронной промышленности (Electronic Industries Association – EIA)

Организация, объединяющая производителей электронного оборудования в США. Регламентирует электрические и функциональные характеристики интерфейсного оборудования и кабельных систем. В 1924 году утвердила **RS-232** - стандарт последовательного соединения с помощью разъемов DB-9 и DB-25 и макс длиной кабеля 15 метров. Определяется соединение между ООД и АПД.

Институт инженеров по электротехнике и радиоэлектронике (ИИЭР) – (Institute of Electrical and Electronic Engineers - IEEE). ИИЭР - международная некоммерческая ассоциация специалистов в области техники, лидер в области разработки стандартов по радиоэлектронике и электротехнике. Эта общественная некоммерческая ассоциация организаций появилась в 1963 году, в результате слияния Института радиотехников (Institute of Radio Engineers, IRE) созданном в 1912 году и Американского института инженеров-электриков (American Institute of Electrical Engineers, AIEE) созданном в 1884 году. IEEE объединяет более 400000 членов из 170 стран.

- IEEE 1284 – параллельный интерфейс
- IEEE 1294 – универсальная последовательная шина – USB (Universal Serial Bus)
- IEEE 1394 – FireWire (i-Link) – последовательная высокоскоростная шина, предназначенная для обмена цифровой информацией между компьютером и другими электронными устройствами.

В 1980 году в IEEE был организован комитет 802 по стандартизации локальных КСПД. Результатом его работы было принятие семейства протоколов, содержащих рекомендации по проектированию нижних уровней сетей. Эти стандарты были созданы путем оценки и стандартизация появившихся технологий и протоколов локальных сетей на основе фирменных стандартов сетей Ethernet, Arcnet и TokenRing.

Комитет IEEE 802 включает следующие подкомитеты:

802.1 – взаимодействие и объединение локальных сетей;
802.2 – Logical Link Control, LLC - управление логической передачей данных;
802.3 – сеть на основе метода доступа CSMA/CD - (Ethernet);
802.4 – сеть на основе метода доступа Token Bus;
802.5 – сеть на основе метода доступа Token Ring;
802.6 – Metropolitan Area Network - региональные сети;
802.7 – широкополосная передача данных;

802.8 – оптоволоконная технология передачи данных;
802.9 – интегрированные сети для передачи речи и данных;
802.10 – безопасность КСПД;
802.11 – беспроводные КСПД;
802.12 – сеть с методом доступа по приоритету запроса (100VG-AnyLAN);
802.16 – широкополосные беспроводные КСПД.

1.3.3. Соответствие модели OSI и модели сетевого взаимодействия TCP/IP

Модель TCP/IP (Модель DOD, Модель DARPA) (Department of Defense – министерство обороны США, DARPA (Defense Advanced Research Projects Agency – агентство передовых оборонных исследовательских проектов) – модель сетевого взаимодействия, разработанная министерством обороны США, практической реализацией которой является стек протоколов TCP/IP. В 1969 году министерство обороны США инициировало работы по объединению суперкомпьютеров оборонных и научно-исследовательских центров в единую сеть на основе пакетной коммутации, протоколы для которой выстраивались в иерархическую модель. Рабочий вариант стека протоколов TCP/IP был создан в конце 70-х годов. Этот стек представлял собой набор базовых протоколов для разнородной вычислительной среды и предназначался для связи экспериментальной сети ARPANET с другими смежными сетями университетов и организаций. В 1983 году стек протоколов TCP/IP был принят министерством обороны США в качестве военного стандарта. В настоящее время протоколы этой модели составляют основу того, что сейчас называется словом Internet. Ретроспектива этой модели дана в документе IETF RFC 871.

TCP/IP – собирательное название для стека сетевых протоколов разных уровней, используемых в Интернет. Стек TCP/IP включает следующие основные протоколы: IP/IPv6 – Интернет протокол; TCP – протокол управления передачей и UDP – протокол пользовательских датаграмм.

Стек протоколов TCP/IP делится на 4 уровня (рис. 1.8):
- прикладной (Application),
- транспортный (Transport),
- межсетевой (Internet),
- физический и канальный (Network Access).

Выделим существенные отличия данных архитектур:

Архитектура ИСО ВОС предусматривает жёсткий набор протоколов на всех уровнях модели, когда на каждом уровне между взаимодействующими объектами сначала устанавливается логическая связь, а уже затем передаются данные. При этом сверху донизу сохраняется последователь-

ность передачи протокольных единиц (блоков, фрагментов, пакетов, кадров) и предпринимаются специальные меры для сохранения целостности этих порций данных. В случае потери или искажения протокольной единицы на каждом уровне (кроме физического) осуществляются перезапрос и повторная передача искажённой протокольной единицы.

Архитектура TCP/IP предусматривает возможность ветвления и добавления новых протоколов. За целостностью данных следит транспортный уровень при использовании протокола TCP, либо сам пользователь при использовании протокола UDP.

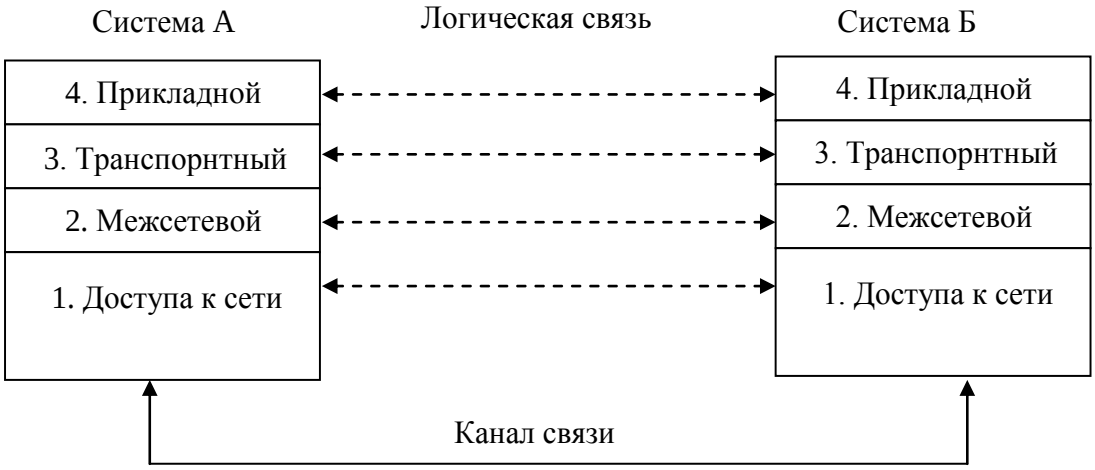


Рис. 1.8. Структура модели протоколов TCP/IP

Переход компьютеров сети ARPANET на стек TCP/IP ускорила его реализация для операционной системы UNIX. Было предложено два интерфейса программирования сетевых приложений: Berkley sockets, реализующий TCP/IP, и интерфейс транспортного уровня TLI (Transport Layer Interface). Интерфейс Berkley sockets был разработан в университете Беркли и использовал стек протоколов TCP/IP. TLI был создан корпорацией AT&T в соответствии с определением транспортного уровня модели OSI и впервые появился в системе System V версии 3. Хотя эта версия содержала TLI и потоки, первоначально в ней не было реализации TCP/IP или других сетевых протоколов, но подобные реализации предоставлялись сторонними фирмами. Позже реализация TCP/IP официально и окончательно была включена в базовую поставку System V версии 4. С этого времени началось совместное существование UNIX и протоколов TCP/IP, а практически все многочисленные версии Unix стали сетевыми.

Взрывной рост количества сетей TCP/IP в конце 90-х годов вызвал то, что семиуровневая модель OSI критиковалась отдельными авторами. В частности, в книге 1998 года «UNIX. Руководство системного администратора» Эви Немет (Evi Nemeth) писала:

Пока комитеты ITU и ISO спорили о своих стандартах, за их спиной менялась вся концепция организации сетей и по всему миру внедрялся протокол TCP/IP.

…

И вот, когда протоколы ISO были наконец реализованы, выявился целый ряд проблем:

эти протоколы основывались на концепциях, не имеющих в современных сетях никакого смысла;

их спецификации были в некоторых случаях неполными;

по своим функциональным возможностям они уступали другим протоколам;

наличие многочисленных уровней сделало эти протоколы медлительными и трудными для реализации.

…

Сейчас даже самые ярые сторонники этих протоколов признают, что OSI постепенно движется к тому, чтобы стать маленькой сноской на страницах истории компьютеров.

1.3.4. Технические компоненты КСПД

Основными компонентами локальных КСПД являются: передающие среды, рабочие станции, интерфейсные платы, серверы. Локальные КСПД могут также подключаться к другим локальным и глобальным телекоммуникационным сетям с помощью специальных устройств сопряжения, реализуемых в виде специализированных устройств или на базе персональных ЭВМ, дооснащенных соответствующими аппаратными и программными средствами. Понимание различий между устройствами сопряжения очень важно, особенно сейчас, когда начинают появляться различного рода гибридные устройства, выполняющие смешанные функции. Существует целый ряд подобных устройств, отличающихся реализуемыми функциями, принципами построения и способами использования:

Мост (Bridge). Мост соединяет два участка сети (сетевых сегмента) и пропускает пакеты в зависимости от их адреса, обеспечивая сопряжение фрагментов локальных КСПД на уровне звена данных ЭМВОС. Оба сегмента должны являться составными частями единой сети передачи данных или локальной вычислительной сети с одним сетевым адресом. Так как мост позволяет объединять различные однотипные сегменты локальных КСПД на подуровне доступа к среде передачи (MAC), то с его помощью можно соединить любые две сети, соответствующие стандарту IEEE 802.2 в не зависимости от различий в средах передачи и методах доступа. Ис-

пользование мостов позволяет обеспечить повышение эффективности, безопасности и протяженности локальных сетей. Многопортовый мост называют **Коммутатором** (Switch).

Маршрутизатор (Router). Маршрутизатор работает на сетевом уровне модели ВОС. Он по адресу пакета определяет один из маршрутов, по которому будет направлен пакет, и обеспечивает соединение между собой (на сетевом уровне) различных фрагментов локальных сетей или отдельных, работающих по различным протоколам локальных вычислительных сетей, каждая из которых имеет свой сетевой адрес. В отличие от мостов, маршрутизаторы являются протокол-ориентированными и их целесообразно применять в больших локальных КСПД. Часто многопротокольные маршрутизаторы используются как пограничные устройства для объединения географически удаленных фрагментов локальной сети через территориальную сеть.

Мост-маршрутизатор (Brouter). Это гибрид двух устройств (моста и маршрутизатора), выполняющий отдельные функции как одного, так и другого устройства. Он реализует функции уровня звена данных и сетевого уровня, обеспечивая фильтрацию и маршрутизацию поступающих пакетов, являясь подобно мосту протокол-неориентированным устройством. Многопортовые варианты такого устройства называют **коммутаторами третьего уровня.**

Шлюз (Gateway). Это устройство, предназначенное не только для соединения отдельных сетей, но и для трансляции (преобразования) и согласования протоколов соединяемых сетей из одного в другой и обратно. Шлюзы работают на всех семи уровнях модели ВОС.

Репитер, **повторитель** (Repeater). В отличие от вышеперечисленных устройств репитер работает на самом нижнем уровне модели ВОС - физическом. Он может только принимать и отправлять пакеты, обеспечивая лишь электрическое сопряжение двух подсетей. Репитер регенерирует принятый сигнал и позволяет увеличить расстояние, на которое может быть передан сигнал. Все вышеперечисленные устройства также обеспечивают выполнение функций репитера.

Концентратор (Hub), как следует из названия, служит для объединения в сеть нескольких сегментов. Концентраторы представляют собой несколько собранных в едином конструктиве репитеров, и они выполняют те же функции, что и репитеры (рис.1.9).

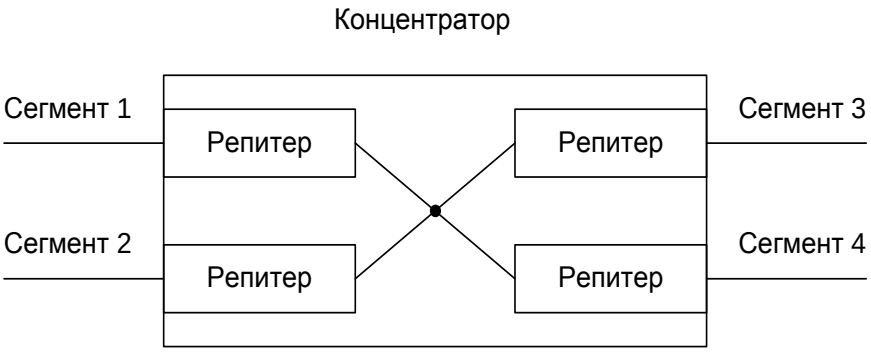


Рис.1.9. Структура концентратора

Преимущество подобных концентраторов по сравнению с отдельными репитерами в том, что все точки подключения собраны в одном месте, это упрощает реконфигурацию сети, контроль и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого источника питания.

Концентраторы иногда вмешиваются в обмен, помогая устранять некоторые явные ошибки обмена. В любом случае они работают на первом уровне модели ВОС, так как имеют дело только с физическими сигналами, с битами пакета и не анализируют содержимое пакета, рассматривая пакет как единое целое (рис.1.10). Концентраторы и репитеры работают на первом уровне модели ВОС.

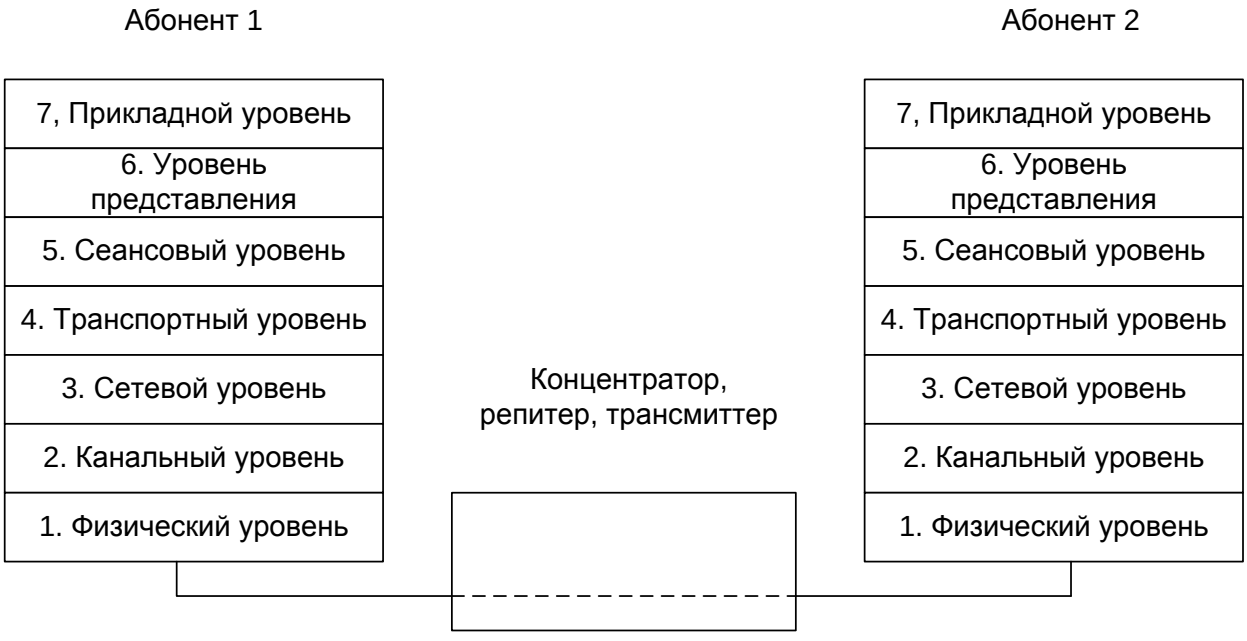


Рис.1.10. Функции концентраторов, репитеров в модели ВОС

Сетевые адаптеры (NIC – Network Interface Card), они же контроллеры, карты, платы, интерфейсы. Это основная часть аппаратуры локаль-

ной сети. Назначение сетевого адаптера – сопряжение РОС, компьютера или другого устройства с сетью, то есть обеспечение обмена информацией между узлом и каналом связи в соответствии с принятыми правилами обмена. Именно они реализуют функции двух нижних уровней модели ВОС. Как правило, сетевые адаптеры выполняются в виде платы, вставляемой в слоты расширения системной магистрали (шины) компьютера (чаще всего PCI или PC-Card). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

Функции сетевого адаптера делятся на магистральные и сетевые. К магистральным относятся те функции, которые осуществляют взаимодействие адаптера с магистралью (системной шиной) компьютера (то есть опознание своего магистрального адреса, пересылка данных в компьютер и из компьютера, выработка сигнала прерывания работы компьютера и т.д.). Сетевые функции обеспечивают общение адаптера с сетью.

К основным сетевым функциям адаптеров относятся:

– гальваническая развязка компьютера и кабеля локальной сети, для чего обычно используется подключение к среде через импульсные трасформаторы;
– преобразование логических сигналов в сетевые (электрические или световые) и обратно;
– кодирование и декодирование сетевых сигналов;
– опознавание принимаемых пакетов, т.е. выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно;
– буферирование передаваемой и принимаемой информации в буферной памяти адаптера;
– организация доступа к сети в соответствии с принятым методом управления обменом;
– подсчет контрольной суммы кадров при приеме и передаче.

Типичный алгоритм взаимодействия ЭВМ с сетевым адаптером выглядит следующим образом.

Если ЭВМ хочет передать сообщение по КСПД, то она сначала формирует этот пакет в своей памяти, затем пересылает его в буферную память сетевого адаптера и дает команду сетевому адаптеру на передачу. Адаптер анализирует текущее состояние сети и при первой же возможности выдает пакет в сеть, т.е. выполняет управление доступом к сети. При этом он производит преобразование информации из буферной памяти в последовательный вид для побитной передачи по сети, подсчитывает контрольную сумму, кодирует биты пакеты в сетевой код и через узел гальванической развязки выдает пакет в кабель сети. Буферная память в данном случае позволяет освободить компьютер от контроля состояния сети, а также обеспечить требуемый для сети темп выдачи информации.

Если по сети приходит кадр, то сетевой адаптер через узел гальванической развязки принимает биты пакета, производит их декодирование из сетевого кода и сравнивает сетевой адрес приемника из пакета со своим собственным адресом. Адрес сетевого адаптера, как правило, устанавливается производителем адаптера. Если адрес совпадает, то сетевой адаптер записывает пришедший пакет в свою буферную память и сообщает сетевой операционной системе (обычно – сигналом аппаратного прерывания) о том, что пришел кадр. Одновременно с записью кадра производится подсчет контрольной суммы, что позволяет к концу приема сделать вывод, имеются ли ошибки в этом кадре. Буферная память в данном случае позволяет освободить ЭВМ от контроля сети, а также обеспечить высокую степень готовности сетевого адаптера к приему пакетов.

Чаще всего сетевые функции выполняются специальными микросхемами высокой степени интеграции, что дает возможность снизить стоимость адаптера и уменьшить размер платы.

Некоторые адаптеры позволяют реализовать функцию удаленной загрузки, то есть поддерживать работу в сети бездисковых ЭВМ, загружающих свою операционную систему прямо из сети. Для этого в состав таких адаптеров включается постоянная память с соответствующей программой загрузки.

Сетевой адаптер выполняет функции первого и второго уровней модели ВОС.

1.4. Классификация КСПД

Для классификации компьютерных сетей используются различные признаки, но чаще всего сети делят на типы по территориальному признаку, то есть по величине территории, которую покрывает сеть. И для этого есть веские причины, так как отличия технологий локальных и глобальных сетей очень значительны, несмотря на их постоянное сближение.

Глобальные сети – Wide Area Networks (WAN) – объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах.

Городские сети (или сети мегаполисов) – Metropolitan Area Networks (MAN) – являются сравнительно недавно появившимися. Они предназначены для обслуживания территории крупного города – мегаполиса. Сети мегаполисов предназначены для связи локальных сетей в масштабах города и доступа локальных сетей к глобальным.

К **локальным сетям** – Local Area Networks (LAN) – относят сети компьютеров, сосредоточенные на небольшой территории (обычно в радиусе не более 1-2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

В зависимости от того, как распределены функции между компьютерами сети, локальные сети делятся на два класса: одноранговые и многоранговые. Последние чаще называют сетями с выделенными серверами.

Если РОС предоставляет свои ресурсы (сервисы) другим пользователям сети, то он играет роль **сервера**. При этом РОС, обращающийся к ресурсам другой машины, т.е. заказчик услуг, является **клиентом**. Как уже было сказано, РОС, работающий в сети, может выполнять функции либо клиента, либо сервера, либо совмещать обе эти функции. Сетевая архитектура, в которой задания или сетевая нагрузка распределены между серверами, и клиентами называется клиент-серверной.

Одноранговые сети — это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел является как клиентом, так и сервером. В одноранговых сетях на всех компьютерах устанавливается такая операционная система, которая предоставляет всем компьютерам в сети потенциально равные возможности. Сетевые операционные системы такого типа называются одноранговыми.

Одноранговые сети проще в развертывании и эксплуатации; по этой схеме организуется работа в небольших сетях, в которых количество РОС, в качестве которых обычно выступают персональные ЭВМ, не превышает 10-20. В этом случае нет необходимости в применении централизованных средств администрирования - нескольким пользователям нетрудно договориться между собой о перечне разделяемых ресурсов и паролях доступа к ним.

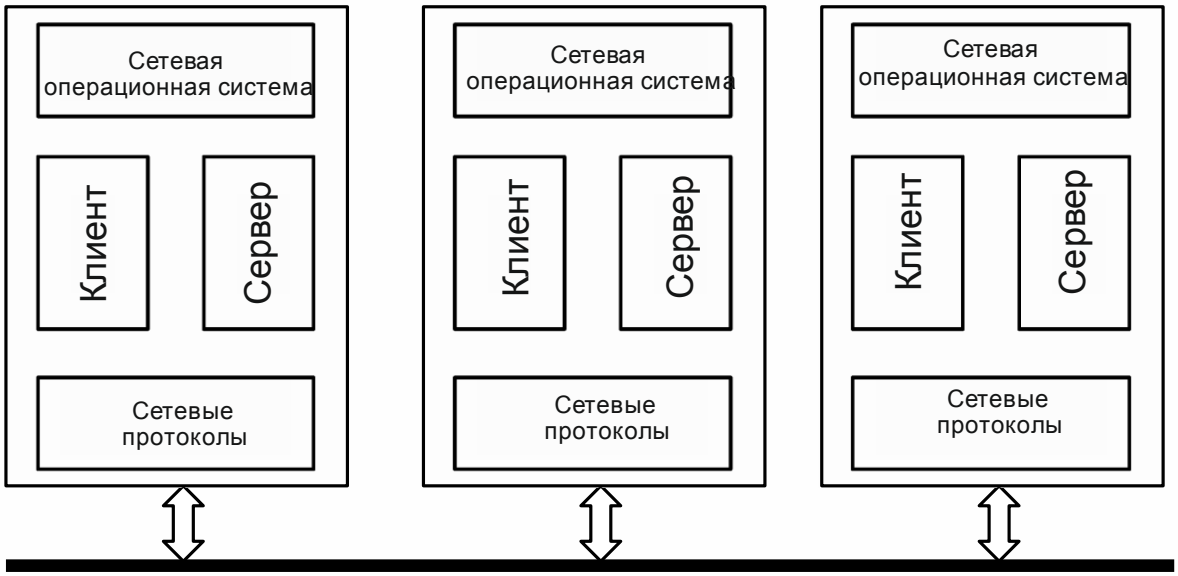


Рис.1.11. Одноранговая локальная сеть

Если выполнение каких-либо серверных функций является основным назначением одного или нескольких узлов сети (например, предоставление

файлов в общее пользование всем остальным пользователям сети или организация совместного использования факсимильной связи), то такой компьютер называется выделенным сервером.

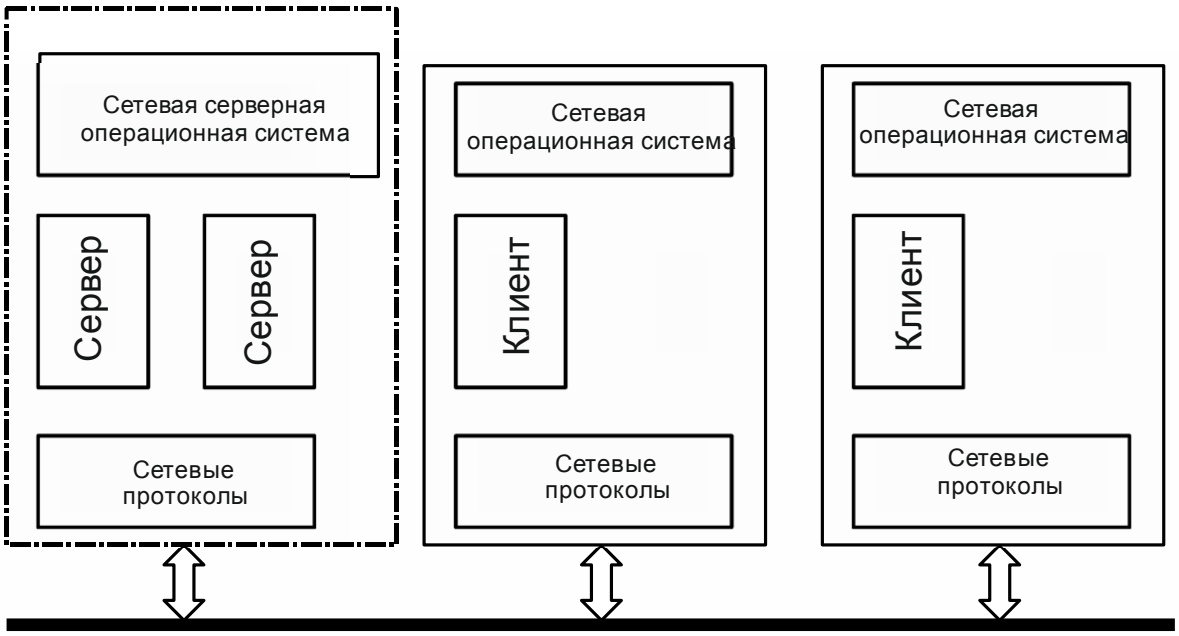


Рис.1.12. Многоранговая локальная сеть

В сетях с выделенными серверами используются специальные варианты сетевых операционных систем, которые оптимизированы для работы в роли серверов и называются серверными операционными системами. Пользовательские компьютеры в таких сетях работают под управлением клиентских операционных систем.

1.5. Топология физических связей

Сеть, состоящая из трех и более компьютеров, должна иметь определенную структуру. Это означает, что все машины, входящие в нее, должны быть физически связаны между собой по какому-либо принципу. Принцип (метод) организации соединений между компьютерами в сети называется **топологией.**

Схематично топология сети изображается с помощью графа, в котором в роли вершин выступают узлы сети (компьютеры, коммутаторы или концентраторы), а в роли ребер – кабель, соединяющий эти узлы, т. е. физическая связь.

Следует различать понятия **физической** и **логической** топологий. В первом случае имеются в виду непосредственно электрические соединения кабелем между машинами. Логические же связи, определяемые настройками маршрутизации оборудования сети, характеризуют путь (маршрут), по которому будет происходить обмен информацией между компьютерами.

От выбора той или иной топологии во многом зависят следующие характеристики сетей: масштабируемость сети, состав коммутационного оборудования и его технические характеристики (быстродействие, количество портов и т. д.), метод управления сетью, стоимость построения и эксплуатации сети, тип физической среды (разновидность кабеля, способ его прокладки, максимальная длина кабеля между узлами), способ взаимодействия между компьютерами.

Например, простая топология позволяет легко масштабировать и расширять сеть. Сложная топология с наличием обходных путей между узлами, резервных соединений повышает надежность, работоспособность сети, но при этом плохо масштабируется, т. к. необходимо много избыточных связей. С экономической же точки зрения наиболее выгодной будет топология с минимальным числом связей. Таким образом, в каждом конкретном случае необходимо выбирать такую топологию, которая лучше всего соответствует выдвигаемым требованиям.

В **полносвязной** топологии (рис. 1.13, а) компьютеры связаны между собой по принципу «каждый с каждым». Для каждой пары компьютеров должна быть выделена отдельная физическая линия связи. В некоторых случаях две, если невозможно использование этой линии для двусторонней передачи. Полносвязные топологии в крупных сетях применяются редко, так как для связи *N* узлов требуется *N*(N-1)/2* физических дуплексных линий связей, то есть имеет место квадратичная зависимость от числа узлов. Чаще этот вид топологии используется в многомашинных комплексах или в сетях, объединяющих небольшое количество узлов.

Достоинством этого типа является простота логики построения, а недостатком – избыточность связей, низкая эффективность и неэкономичность. Такую топологию применяют в сетях с небольшим количеством узлов.

Все другие варианты основаны на неполносвязных топологиях, когда для обмена данными между двумя компьютерами может потребоваться транзитная передача данных через другие узлы сети.Если из полносвязной топологии убрать часть связей, соединив напрямую только те компьютеры, между которыми передается большой объем данных, то получится *ячеистая* топология (рис. 1.13, б). При этом передача данных между узлами, не имеющими прямого соединения также возможна, но только через транзитные узлы. Такую топологию часто используют в глобальных сетях, с ее помощью можно соединить большое количество машин.

Топология, при которой все узлы подключаются к одному сегменту кабеля (магистрали), называется **общей шиной** (рис. 1.13, в). Очевидно, что главным достоинством ее является дешевизна. Такой способ построения сети обеспечивает возможность быстрой рассылки широковещательного трафика, простоту присоединения узлов к сети. Одним из основных недостатков является невозможность передачи данных в сеть несколькими

машинами одновременно, они вынуждены передавать данные по очереди. Отсюда возникают проблемы, связанные с организацией доступа к сети так, чтобы все узлы могли передавать информацию с задержкой, не выше допустимой, и пропускная способность сети была использована по максимуму, без простоев. Также из-за последовательного соединения компьютеров топология обладает низкой надежностью, т. к. при неисправности любого участка сети (дефект кабеля, разъема для подключения) приводит к выходу из строя всей сети сразу.

При топологии **звезда** (рис. 1.13, г) все узлы подключаются кабелем к концентратору, который находится в центре. К плюсам этой топологии можно отнести повышение надежности сети за счет использования отдельных сегментов кабеля для подключения компьютером. Т.е. если неисправен какой-то разъем машины или кабель, с помощью которого она подключена к концентратору, то это не повлияет на работу остального оборудования. Однако это является и минусом, поскольку увеличение суммарной длины кабеля приведет к росту стоимости сети. Сама необходимость концентратора в структуре сети также увеличивает затраты. К тому же, при его выходе из строя будет нарушена работоспособность всей сети. Количество узлов при данной топологии ограничено числом портов концентратора. Частично эта проблема решается применением нескольких концентраторов, которые между собой также соединяются по топологии звезда (рис. 1.13, д).

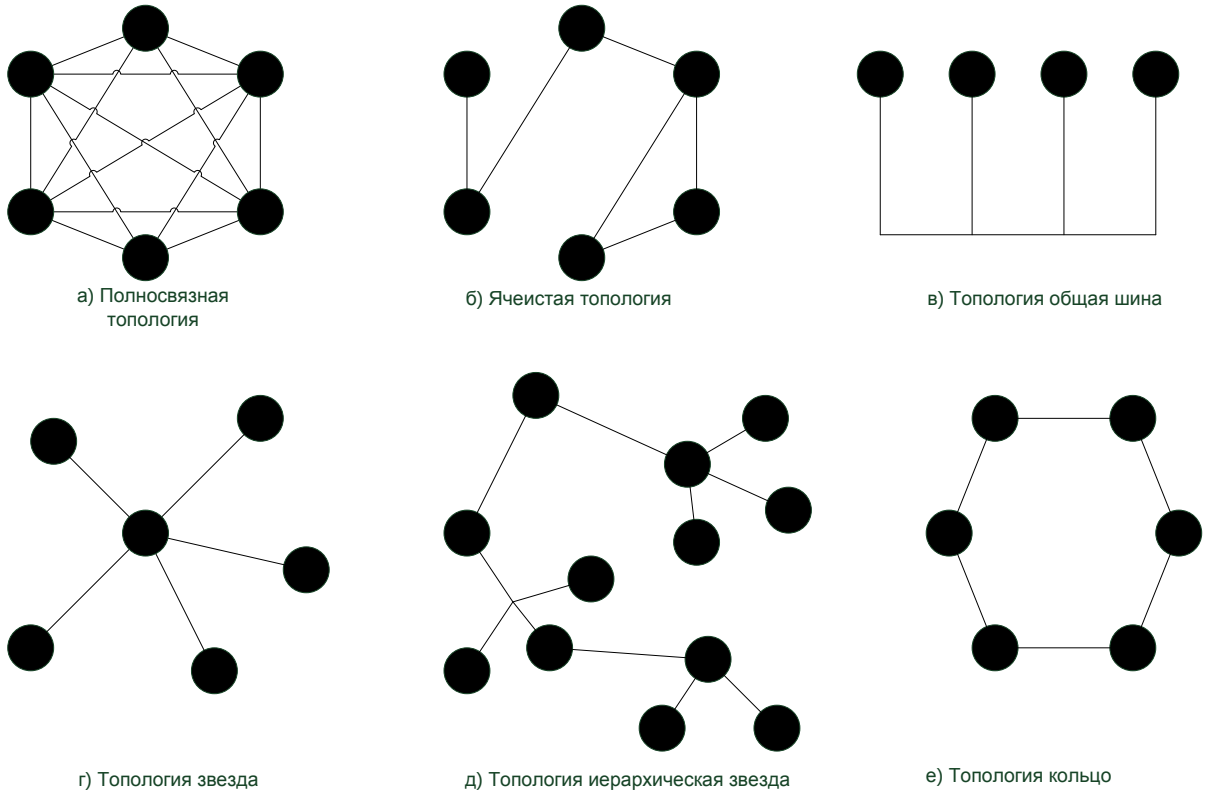


Рис.1.13. Типовые топологии КСПД

Использование концентратора не позволяет осуществлять одновременную передачу ему данных от нескольких компьютеров, иначе возникает коллизия. Решить эту проблему можно заменой концентратора на коммутатор. Он, в отличие от концентратора, передает кадры не на все остальные порты (за исключением того, на который поступил кадр), а только на порт получателя. Определение нужного порта происходит за счет аппаратного адреса получателя. С помощью коммутатора также можно фильтровать данные, которые поступают от компьютеров в сеть, блокировать какие-либо передачи. Топология звезда является одной из самых распространенных в глобальных и локальных сетях.

Топология **кольцо** (рис. 1.13, е) подразумевает передачу данных от одного узла к другому последовательно. Если на узел поступили данные, и он определил, что они предназначены для него, то он копирует их во внутренний буфер, а если нет, то передает дальше по кольцу. К достоинствам данной топологии можно отнести наличие двух путей между каждой парой узлов – по часовой стрелке и против нее. Надежность также можно повысить созданием «двойного кольца» (как в технологии FDDI). При этом будет происходить переключение на резервное кольцо в случае неисправности основного. В кольцевой структуре легко можно организовать обратную связь, поскольку при прохождении всего кольца кадр вновь возвращается к узлу-отправителю. Одним из недостатков такой организации сети является ограниченность количества узлов. Компьютеры не могут передавать данные по кольцу одновременно, только в порядке очереди, а поэтому при большом числе узлов задержки при передаче кадров будут недопустимыми.

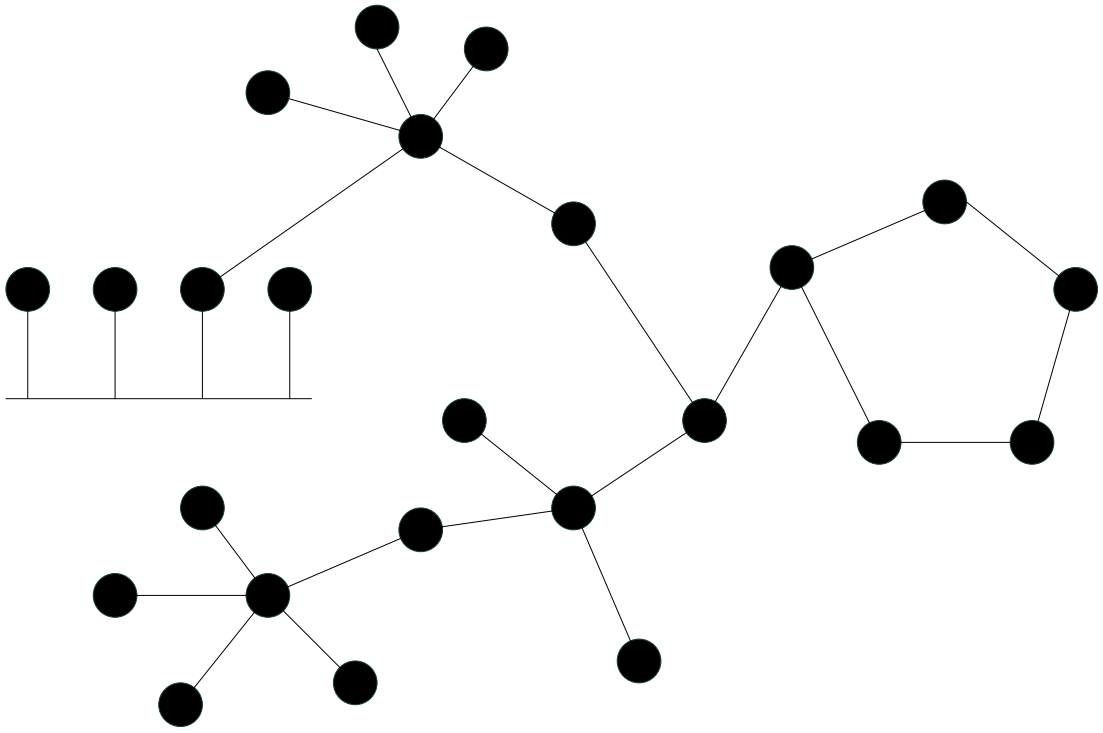


Рис. 1.14. Смешанная топология

Во всех базовых топологиях число включаемых в сеть машин очень ограничено. Поэтому в крупных, глобальных сетях, как правило, в чистом виде ни одна из них не применяется, а используется *смешанная топология* (рис. 1.14). Она представляет собой совокупность отдельных фрагментов сети с базовыми топологиями, произвольным образом соединенных между собой.

1.5.1. Зависимость топологий от особенностей физической среды передачи

Использование в сетях помимо индивидуальных, еще и разделяемых линий связи, когда они используются компьютерами по очереди, порождает целый ряд проблем. Во-первых, при подключении к одному кабелю нескольких машин необходимо обеспечивать необходимое качество передачи данных (электрических сигналов). Во-вторых, нужно осуществлять еще и логическое разделение по времени моментов передачи информации от каждого узла сети. При использовании разделяемых линий всегда теряется производительность, т.к. пропускная способность линии распределяется между всеми узлами сети, в отличие от индивидуальной линии, вся пропускная способность которой используется одним узлом. Но, несмотря на это, разделяемые линии используются довольно часто из-за экономии, например, в технологиях Ethernet (включая Fast Ethernet и Gigabit Ethernet), Token Ring.

За экономию средств на построение сети приходится платить производительностью. Поэтому в локальных сетях наряду с разделяемыми линиями используются и индивидуальные. Например, в звездообразной топологии узлы подключаются к коммутаторам с помощью индивидуальных линий, а коммутаторы между собой соединяются разделяемыми (рис. 1.15). Однако в глобальных сетях разделяемые линии применять нельзя. Иначе задержки сигналов могут стать недопустимо высокими, вплоть до того, что машинам придется дольше решать вопрос о порядке доступа, чем непосредственно передавать данные.

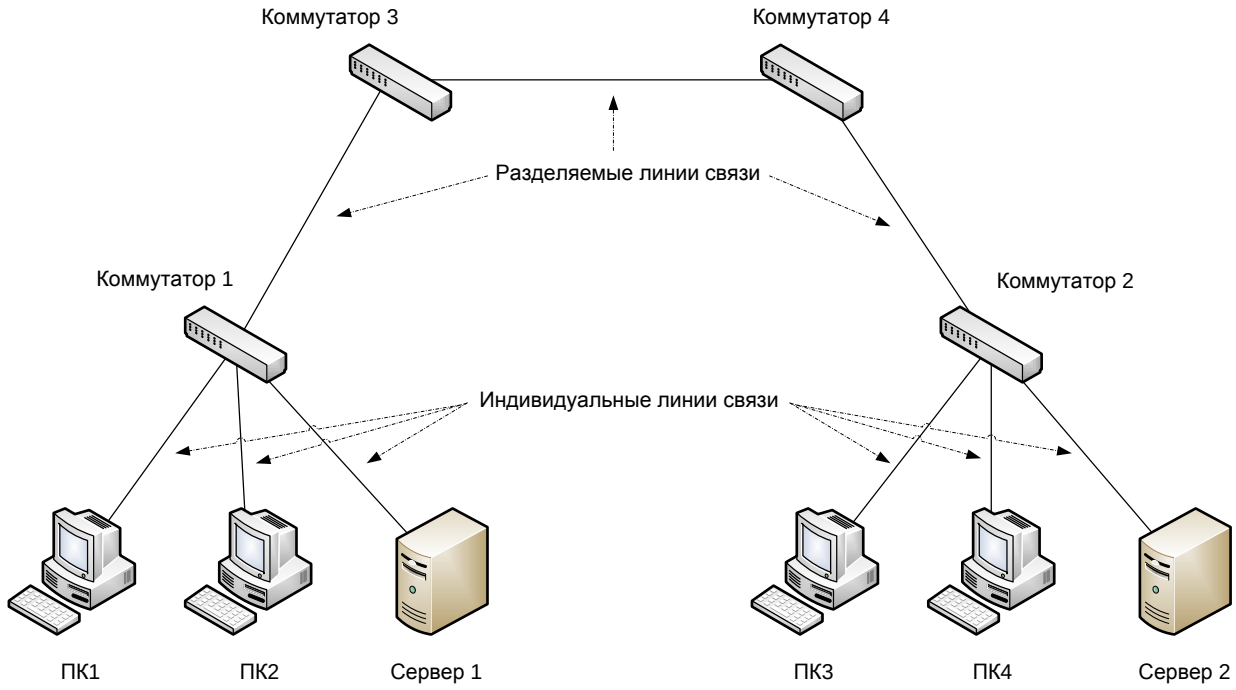


Рис. 1.15. Разделяемые и индивидуальные линии связи в сетях на основе коммутаторов

В крупных сетях однородность структуры связей, характерная для базовых топологий, становится минусом, а не плюсом. В силу особенностей физической среды передачи данных при использовании базовых топологий возникают следующие ограничения:

- на количество машин в сети;
- на количество коммуникационного оборудования;
- на длину кабеля между различными узлами сети;
- на интенсивность порождения трафика узлами.

Частично проблему этих ограничений можно решить с помощью физической и логической структуризации сети.

Физическую структуризацию обеспечивает коммуникационное оборудование, например, концентраторы. *Концентратор* (или *хаб*) – это устройство, имеющее несколько портов для подключения сегментов сети и обеспечивающее обмен данными между ними. Сигнал при прохождении по кабелю подвергается затуханию и различного рода искажениям. Поэтому длина кабеля, соединяющего какие-либо два узла в сети, ограничена. Концентратор выступает в роли регенератора, т. е. обеспечивает восстановление поступающего на один из портов сигнала по амплитуде, мощности и фазе, тем самым позволяя увеличить общий размер сети, и передает его на другие порты.

Во всех технологиях принцип работы концентратора по сути одинаков. В Ethernet, например, восстановленный сигнал передается на все порты, кроме входящего (рис. 1.16, а), а в Token Ring с кольцевой топологией – на тот, к которому подключается следующий узел в кольце

(рис. 1.16, б). При этом концентратор меняет только физическую топологию, логические же связи в сети остаются прежними. Но совсем необязательно физическая и логическая топология будут отличаться, в частном случае они могут и совпадать.

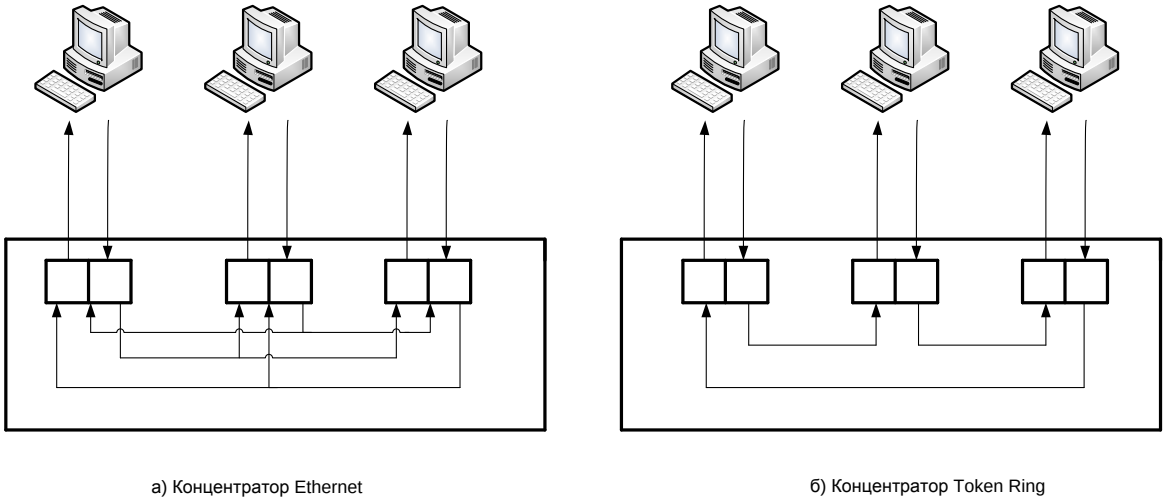


Рис. 1.16. Концентраторы (хабы) различных технологий

Кроме борьбы с вышеперечисленными ограничениями, физическая структуризация позволяет сделать сеть более надежной. Концентратор может автоматически отключать порт, когда на него поступает нежелательный трафик или когда один узел начинает непрерывно передавать кадры в сети (в Ethernet).

Логическая структуризация помогает решить задачу распределения потоков данных между различными сегментами сети. Допустим, имеется какая-то большая организация, состоящая из нескольких отделов. Сеть в такой организации также будет логически разделена на подсети по имеющимся отделам. Соответственно, сотрудники одного отдела будут обмениваться информацией как между собой, так и с коллегами из других отделов. Причем, вероятнее всего, объем внутреннего трафика отдела будет выше, чем объем внешнего (между разными отделами). Если строить сеть по одной из базовых топологий (общая шина, звезда или кольцо) и рассматривать ее как одну разделяемую среду, то при большом числе машин пропускная способность в расчете на один узел будет мизерной.

В таком случае рациональнее логически разделить сеть на сегменты и распространять данные, предназначенные для машин одного сегмента, лишь в пределах этого сегмента, т.е. локализовать трафик.

Логическая структуризация сети может осуществляться с помощью коммутаторов и маршрутизаторов. *Коммутатор* делит сеть на логические сегменты, передавая данные между ними только тогда, когда получателем является узел другой подсети (рис. 1.17, а). В этом случае принадлежность узла к той или иной подсети полностью определяется его аппаратным адресом. Локализация трафика позволяет увеличить производительность сети

путем экономии пропускной способности каналов, а также обеспечивает конфиденциальность информации, т.к. она распространяется только внутри нужного сегмента.

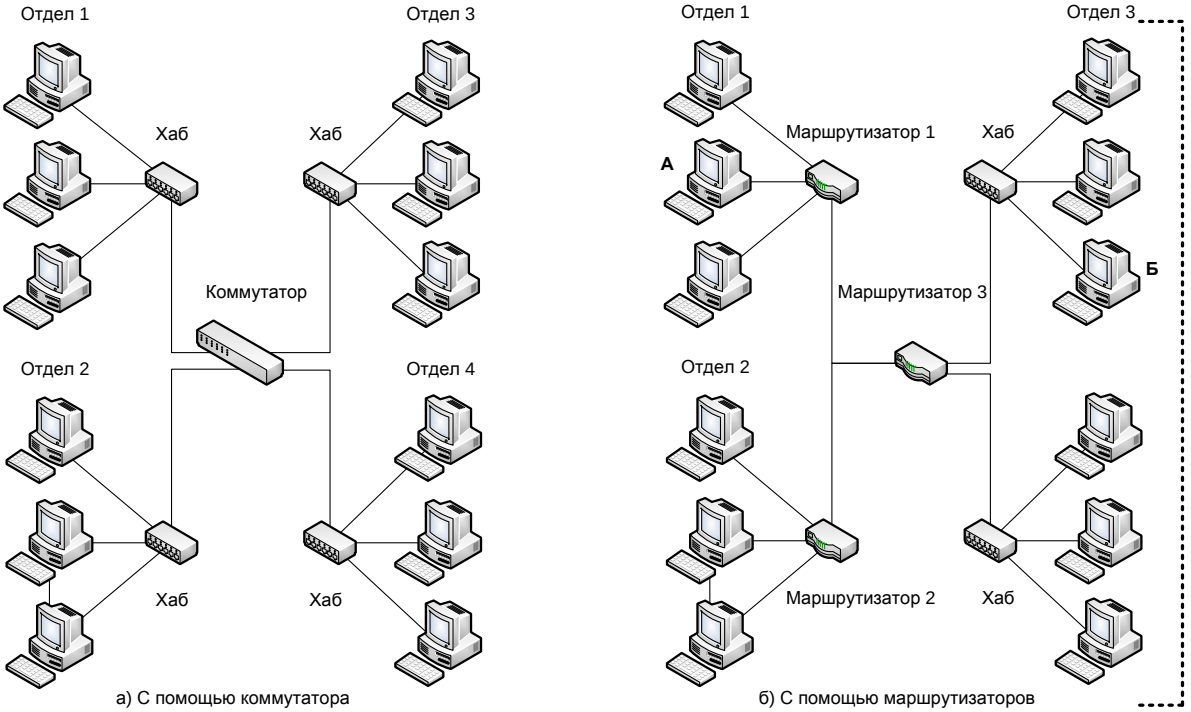


Рис. 1.17. Логическая структуризация сети

Коммутатор может обрабатывать потоки кадров параллельно, то есть обработка данных, поступающих на один порт, не зависит от аналогичных процессов на других портах. Однако коммутатор не имеет информации о точной топологии связей между сетевыми сегментами. Он запоминает порт, на который поступили данные от узла, и использует его для обратной передачи информации, предназначенной для этого узла. Принцип действия коммутаторов не допускает в сети наличия петель, иначе путь трафика замкнется и он будет засорять сеть. Это накладывает ограничения на физическую структуру сети, лишает возможности использовать резервные связи для повышения ее надежности.

Подобные проблемы можно решить с помощью маршрутизаторов (рис. 1.17, б). Они делят сеть на логические сегменты, лучше изолируя трафик между ее частями. Для того, чтобы определить, куда направить поступившие данные, маршрутизатор использует явную адресацию, не аппаратные адреса, а сетевые (IP-адреса). В сетевой адрес входит адрес подсети и адрес хоста, поэтому все узлы, имеющие один и тот же адрес подсети, находятся в одном сегменте. Маршрутизаторы также способны работать в сетях, топология которых содержит петли. При этом в качестве пути для данных выбирается более выгодный маршрут (кратчайший в отношении

времени прохождения по нему данных). За счет использования единой для всех подсетей адресации, маршрутизаторы могут объединять подсети с разными технологиями в единую сеть.

Вопросы

1. Чем можно объяснить тот факт, что глобальные сети появились раньше, чем локальные?
2. Всякое ли приложение, выполняемое в сети, можно назвать сетевым?
3. Как называются сети, перекрывающие территорию не более 10 $м^2$?
4. Как называются сети, расположенные на территории города или области?
5. Как называются сети, расположенные на территории государства или группы государств?
6. Объясните структуру стека протоколов TCP/IP.
7. Сравните две эталонные модели TCP/IP и BOC по числу и назначению уровней.
8. Что общего и в чем отличие между взаимодействием компьютеров в сети и взаимодействием компьютера с периферийным устройством?
9. Как распределяются функции между сетевым адаптером и его драйвером?
10. Поясните значения терминов «клиент» и «сервер»
11. В чем состоит основная особенность кода Манчестер-II?
12. Изобразить, как будут представлены биты в физическом канале передачи данных при цифровом кодировании кодом Манчестер-II:
    а) 111111
    б) 1101011
    в) 0110101
13. Изобразить, как будут представлены биты в физическом канале передачи данных при цифровом кодировании кодом NRZI
    а) 111111
    б) 1101011
    в) 0110101
14. Определите скорость передачи линейного сигнала (В, Бод) при манчестерском кодировании, если скорость передачи информации составляет N=64Кбит/с:
    а) 131072 Бод
    б) 65536 Бод
    в) 64 Кбод
    г) 128 Кбод
15. Назовите главные недостатки полносвязной топологии, а также топологий типа общая шина, звезда, кольцо.
16. Какую топологию имеет односегментная сеть Ethernet, построенная на основе концентратора – общая шина или звезда?

17. Какие из следующих утверждений верны:
    а) разделение линий связи приводит к повышению пропускной способности канала,
    б) конфигурация физических связей может совпадать с конфигурацией логических связей;
    в) главной задачей службы разрешения имен является проверка сетевых имен и адресов на допустимость;
    г) протоколы без установления соединений называются также дейтаграммными протоколами.
18. Определите функциональное назначение основных типов коммуникационного оборудования – повторителей, концентраторов, мостов, коммутаторов, маршрутизаторов.
19. В чем отличие логической структуризации сети от физической?
20. Что такое «открытая система»? Приведите примеры закрытых систем.
21. Поясните разницу в употреблении терминов «протокол» и «интерфейс» применительно к многоуровневой модели взаимодействия устройств в сети.
22. Что стандартизует модель ВОС?
23. Что стандартизует стек модели ВОС?
24. Почему в модели ВОС семь уровней?
25. Дайте краткое описание функций каждого уровня и приведите примеры стандартных протоколов для каждого уровня модели ВОС.
26. Являются ли термины «спецификация» и «стандарт» синонимами?
27. Какая организация разработала основные стандарты сетей Ethernet и Token Ring?
28. Зачем нужен заголовок в протокольных блоках данных ЭМВОС?
29. В чем состоит отличие локальных сетей от глобальных на уровне служб? На уровне транспортной системы?
30. Назовите наиболее часто используемые характеристики производительности сети?

РАЗДЕЛ 2. ПРОТОКОЛЫ ФИЗИЧЕСКОГО И КАНАЛЬНОГО УРОВНЕЙ В ЛОКАЛЬНЫХ КСПД

2.1. История появления локальных сетей

Первой развернутой локальной сетью считается система, построенная в Гавайском университете, под руководством Нормана Абрамсона. Строительство было начато в 1968 г. и закончено в 1971 г. Сеть была названа ALOHAnet или просто ALOHA. Она использовалась для доступа к центральной ЭВМ, расположенной на острове Оаху, пользователями с других островов Гавайского архипелага. Поэтому сеть была построена на радиоканалах, прием центральный узел осуществлял на частоте 417 Мгц а передачу – на частоте 413 Мгц, причем узлы передавали пакеты по общему каналу. Узлы сети ALOHA передавали пакеты со скоростью 9600 бит/с. Сеть имела топологию – звезда.

В 1973 году Роберт Меткалф и Давид Боггс (R. Metcalfe, D. Boggs) в исследовательском центре PARC (Palo Alto Research Centre) фирмы Xerox создали первую ЛВС Ethernet, которая работала со скоростью 2,944 Мбит/с и соединяла два компьютера. Эти компьютеры имели собственные имена «Майкельсон» и «Морли» - по имени двух ученых XIX века, доказавших, что «эфира» (ether) не существует.

По аналогии с законом Мура (Gordon Moore, сооснователь Intel), Меткалф сформулировал, так называемый, закон Меткалфа, служивший верой и правдой, когда надо было обосновать необходимость создания ЛВС: стоимость ЛВС с ростом числа узлов растет линейно, а ценность - пропорционально квадрату числа узлов. Меткалф предсказал экспоненциальный рост сетей.

В 1979 г. в США три фирмы - Xerox, DEC и Intel - объединили свои усилия, чтобы стандартизовать Ethernet в рамках IEEE. Произошло это при посредничестве Боба Меткалфа, который в этом же году с помощью фирмы DEC основал компанию 3Com (тройная аббревиатура от COMputer COMmunications COMpability - совместимость компьютерных коммуникаций). Объединение усилий для стандартизации многократно увеличивало общий сбыт изделий и повышало прибыль каждой компании.

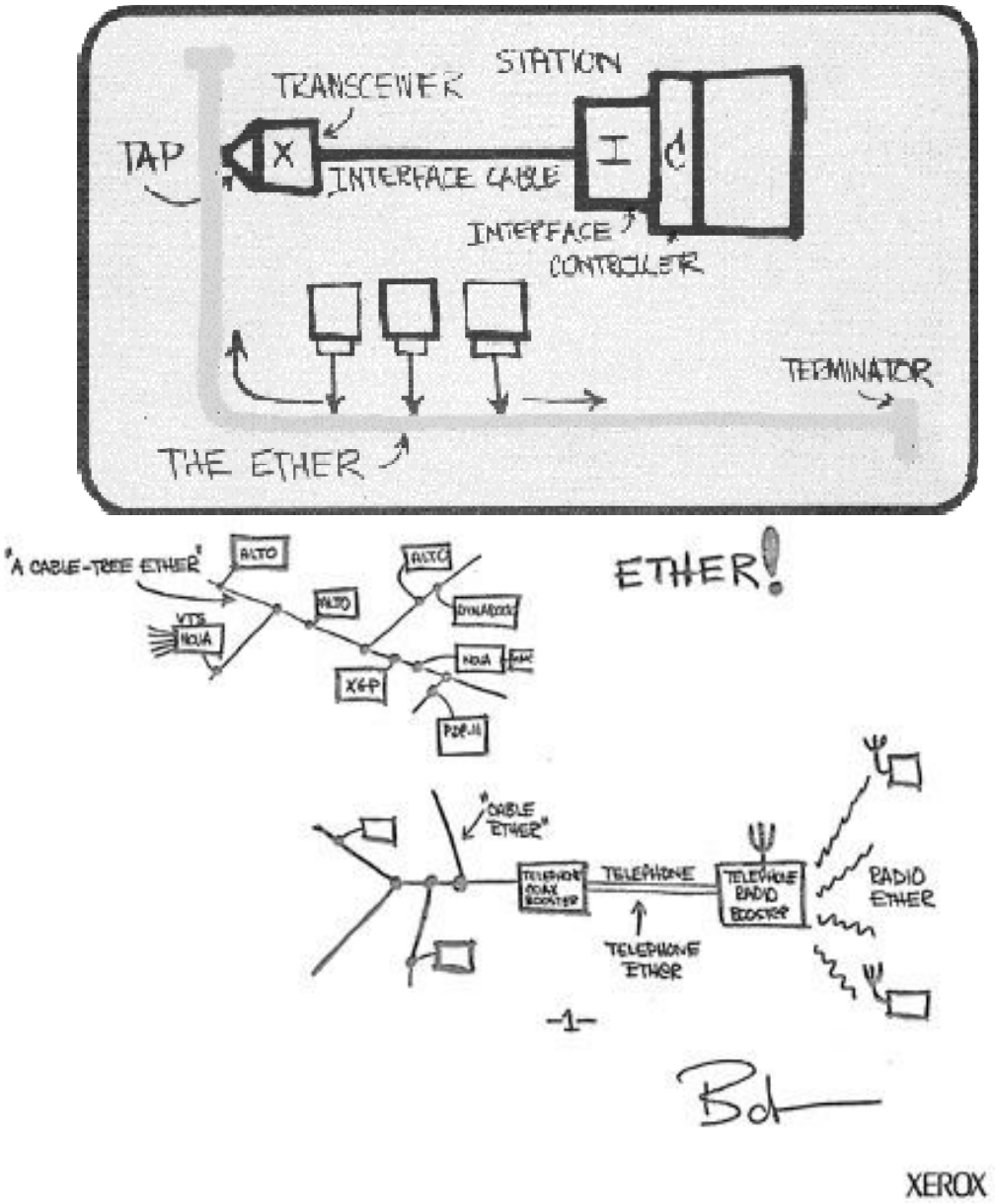


Рис. 2.1. Эскизы технологии Ethernet (Р.Меткалф)

Первые спецификации для сети Ethernet были утверждены IEEE, и получили номер 802.3. В них определялась шинная топология сети 10Base5 (на основе толстого коаксиального кабеля) и 10Base2 (на основе тонкого коаксиального кабеля), скорость передачи 10 Мбит/с, предельное расстояние между точками одного сегмента – 2,5 км.

2.2. Общая характеристика протоколов используемых сетевых технологий в локальных сетях

В 1980 г. в институте инженеров по электротехнике и радиоэлектронике – IEEE был создан комитете 802 с целью разработки стандартов в области локальных КСПД. Подготовка проектов стандартов была возложена на ряд соответствующих подкомитетов. Многие сетевые стандарты IEEE

легли в основу стандартов по локальным КСПД Международной организации по стандартизации и Международной комиссии по электротехнике, которые для этих целей организовали совместный объединённый технический комитет №1 ISO/МЭК (ISO/IEC Joint Technical Committee 1, ISO/IEC JTC 1). Позже результаты работы этого комитета легли в основу комплекса международных стандартов **ISO 8802-1...5.**

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

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

Подкомитеты **802.2** и **802.3**. - **802.5**, опираясь на семиуровневую модель ВОС, выполнили дальнейшую декомпозицию уровней 1 и 2 модели. Согласно модели IEEE уровень звена данных поделен на два подуровня: **управление логическим звеном** (LLC Logical Link Control) и **управление доступом к среде MAC** (Medium Access Control).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень — уровень LLC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг. В современных локальных сетях получили распространение несколько протоколов уровня MAC, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, l00VG-AnyLAN**.**

Уровень LLC отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне

процедур восстановления кадров в случае их потери или искажения, т.е. отличающихся качеством транспортных услуг этого уровня.

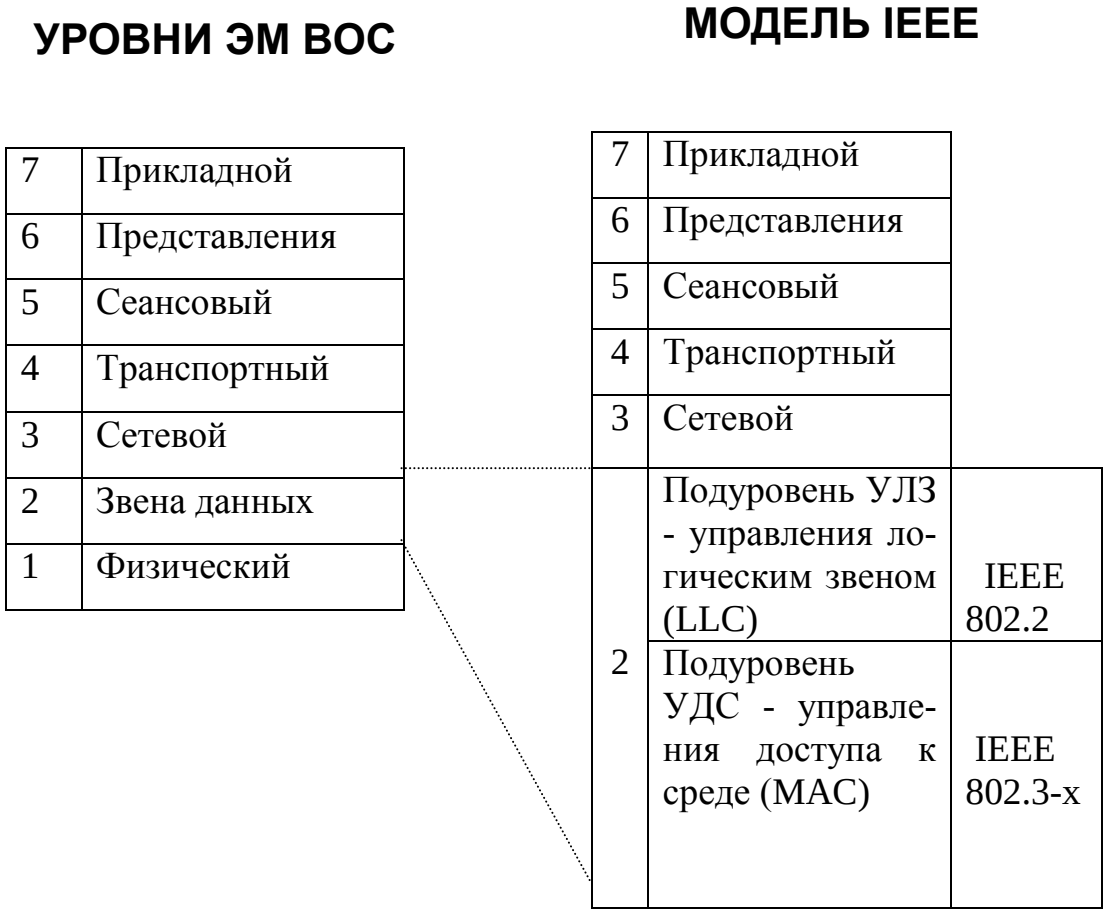


Рис. 2.2. Соотношение уровней ЭМВОС и IEEE для ЛС

Соотношение уровней ЭМВОС и IEEE для локальных КСПД показано на рис. 2.2. В функции протоколов уровня LLC входит передача кадров между станциями (управление потоком данных), включая исправление ошибок. На этом уровне выполняется также диагностика работоспособности узлов локальных КСПД. Способы передачи информации на уровне LLC не зависят от алгоритмов доступа к физической среде и ее типа, если не считать временных параметров.

2.3. Методы доступа к локальным КСПД

Метод доступа к сети определяет алгоритм, согласно которому узлы сети получают доступ к среде передачи данных и осуществляют передачу (включая мультиплексирование / демультиплексирование данных)

В пособии рассмотрены следующие методы доступа:

– ALOHA;
– CSMA/CD;
– CSMA/CA;
– Маркерный доступ.

2.3.1. Метод доступа ALOHA

В сети ALOHAnet или просто ALOHA была звездообразная топология, поскольку эта сеть использовалась для доступа к центральной ЭВМ, расположенной на острове Оаху, пользователей с других островов Гавайского архипелага. Сеть была построена на радиоканалах, прием центральный узел осуществлял на частоте 417 Мгц, а передачу – на частоте 413 Мгц, узлы передавали пакеты по общему каналу. Когда передача от двух узлов происходила одновременно, радиосигналы накладывались и искажали друг друга, т.е. возникали коллизии.

Коллизия (collision — ошибка наложения, столкновение) – наложение двух и более кадров от станций, пытающихся передать кадр в один и тот же момент времени.

В начальной реализации сети ALOHAnet центральный узел подтверждал верно принятые пакеты. Когда узел не получал подтверждение за заранее определённый промежуток времени, он считал, что произошла коллизия и передавал информацию заново. В сети ALOHAnet не использовался контроль несущей, и при обнаружении конфликта передача пакета не прекращалась, поскольку проверка несущей была бесполезна, т.к. узлы размещены далеко друг от друга, и узел мог завершить передачу прежде, чем другой узел обнаружит передачу. По тем же причинам обнаружение коллизий было достаточно долгим. Существует две версии протокола ALOHA: чистая (pure ALOHA) и тактированная, т.е. синхронная (slotted ALOHA). Отличие их в том, что в первой используется модель непрерывного времени, а во второй – дискретного, т.е. тактированного.

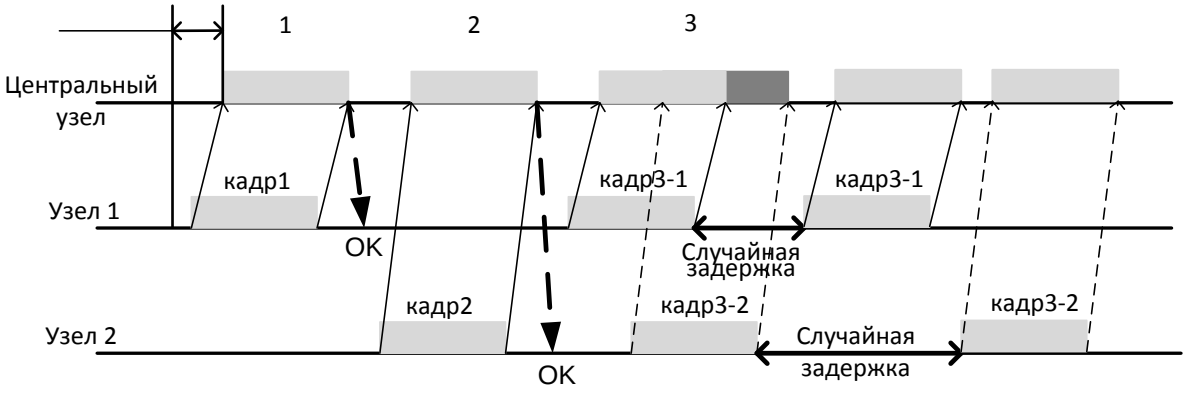


Рис. 2.3. Передача кадров по алгоритму ALOHA

Подведем итог: алгоритм ALOHA использовался для доступа к радиоканалу большого числа независимых узлов, причем отправитель мог

выполнять передачу в любой момент. При этом возможно возникновение коллизий – ситуаций, когда несколько узлов передают одновременно. В случае коллизии сигналы от узлов будут наложены друг на друга и искажены, поэтому получатель должен подтвердить получение данных и сообщить, были ли они искажены в процессе передачи (рис. 2.3). Если данные были искажены, все узлы, одновременно выполнявшие передачу, делают паузу и выполняют повторную попытку через некоторое время, причем размер паузы выбирается случайно.

Для оценки пропускной способности чистого ALOHA, сделаем несколько упрощающих предположений:

1. Все кадры имеют одинаковую длину.
2. Станция не может генерировать новый кадр во время передачи.
3. Поток кадров соответствует распределению Пуассона.

Пусть T – время, необходимое для передачи одного кадра, а G - математическое ожидание, используемое для задания распределения Пуассона, соответствует числу попыток передачи за время T.

t - время, когда мы хотим послать кадр. Т.е. мы начнем использовать канал для передачи одного кадра, начиная с t, и поэтому для успешной доставки все остальные станции должны воздерживаться от передачи в интервал времени t - T, потому что кадр, отправленный в течение этого интервала, будет наложен на наш кадр.

Для любого Т, вероятность наличия k - попыток передачи в течение этого времени составит:

$$G^k e^{-G}/k! \qquad (2.1)$$

Среднее количество попыток передачи в течение 2-х последовательных отрезков времени T составит:

$$(2G)^k e^{-(2G)}/k! \qquad (2.2)$$

Поэтому вероятность P, что количество попыток передачи в течение 2-х последовательных отрезков времени T составит 0, т.е., что передача кадра будет успешна, составит:

$$P = e^{-2G} \qquad (2.3)$$

Пропускная способность может быть рассчитана как умножение попыток передачи на вероятность успеха, и поэтому пропускная способность S будет равна:

$$S = G\, e^{-2G} \qquad (2.4)$$

Таким образом, максимальная пропускная способность $0,5/e$ кадров за время передачи одного кадра (достигается тогда, когда $G = 0.5$), что составляет примерно 0,184 кадров за время передачи одного кадра. Это означает, что при использовании чистого алгоритма ALOHA, только около 18,4% времени используется для успешной передачи кадров.

2.3.2. Метод доступа CSMA/CD

В сетях Ethernet (IEEE 802.3) используется метод доступа к среде передачи данных, называемый метод коллективного доступа с опознаванием несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection - CSMA/CD), который относится к децентрализованным недетерминированным (случайным) методам. Принципиальное отличие от алгоритма ALOHA, с точки зрения распознавания коллизий, заключается в том, что в ALOHA коллизии определяются на входе получателя, а в CSMA/CD – на выходе источника.

Коллизии могут быть обнаружены сравнением передаваемой и получаемой информации на передающей станции. Если она различается, то это значит, что передача кадра от другой станции накладывается на текущую передачу, возникла коллизия, и передача немедленно прерывается, а станция ожидает в течение случайного интервала времени, и затем может снова сделать попытку передачи кадра. Для уменьшения вероятности этой ситуации непосредственно перед отправкой кадра передающая станция прослушивает среду передачи (т.е. принимает и анализирует возникающие на нем электрические сигналы), чтобы обнаружить, не передается ли уже по кабелю кадр данных от другой станции. Если принимается сигнал на несущей частоте, то станция откладывает передачу своего кадра до окончания чужой передачи, и только потом пытается вновь его передать (рис. 2.4).

Несущая частота при манчестерском способе кодирования, принятом для всех вариантов Ethernet 10Base 10 Мбит/с, равна 10 Мгц. Интервал времени до повторной попытки доступа после коллизии определяется как случайное число интервалов отсрочки, где один интервал отсрочки равен 512 битовым интервалам, т.е. 51,2 мкс для передачи со скоростью 10 Мбит/с.

Кадр данных всегда сопровождается преамбулой, которая состоит из 7 байт, каждый из которых имеет значение 10101010, и 8-го байта, равного 10101011. Последний байт носит название ограничителя начала кадра. Преамбула нужна для вхождения приемника в побитовую и побайтовую синхронизацию с передатчиком. Наличие двух единиц подряд говорит о том, что преамбула закончилась и следующий бит является началом кадра.

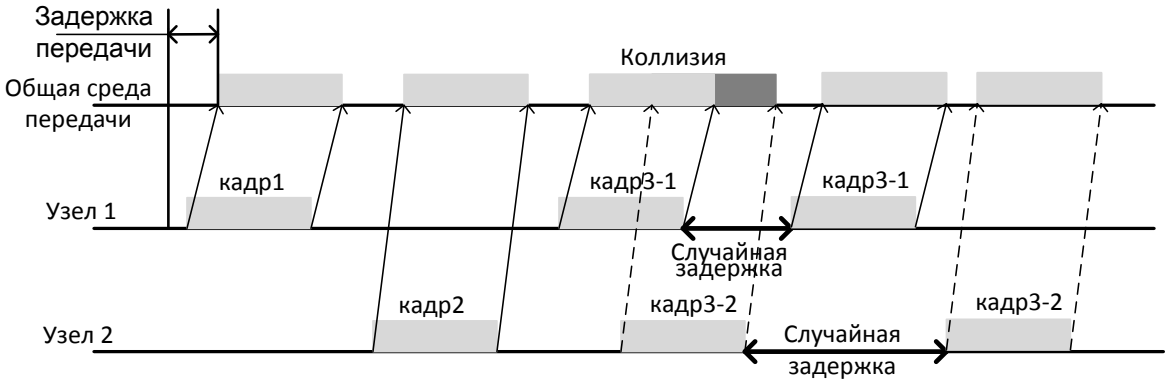


Рис. 2.4. Передача кадров по методу доступа CSMA/CD

Рис. 2.5. Алгоритм CSMA/CD

В случае обнаружения коллизии любым узлом, им же посылается особый сигнал (jam signal), состоящий из 32 бит и представляющий чередование ‘1’ и ‘0’ со стартовым битом ‘1’. Этот сигнал информирует остальные станции о том, что они не должны осуществлять передачу. Это вызывает задержку передачи всех узлов сети на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки передачи своих кадров.

Из описания метода доступа видно, что он носит вероятностный характер, и вероятность успешного получения в свое распоряжение общей

среды зависит от загруженности сети, то есть от интенсивности возникновения в станциях потребности передачи кадров и от количества станций.

Надежное распознавание коллизии является необходимым условием корректной работы сети CSMA/CD. Если какой-либо передающий узел не распознает коллизию и решит, что кадр данных передан им верно, то этот кадр будет утерян. Вероятно, недошедшие данные будут повторно переданы каким-либо протоколом верхнего уровня, например, транспортным, но это произойдет гораздо позже, чем повторная передача средствами канала сети, работающей с микросекундными интервалами. Поэтому если коллизии не будут надежно распознаваться узлами сети CSMA/CD, то это приведет к заметному снижению полезной пропускной способности сети.

Для надежного распознавания коллизий должно выполняться следующее соотношение:

$$T_{min} \geq T_{об}, \qquad (2.5)$$

где T_{min} – время передачи кадра минимальной длины, а $T_{об}$ – время оборота (Path Delay Value), то есть время, за которое сигнал успевает распространиться до самого дальнего узла сети и обратно, так как в наихудшем случае сигнал должен дважды пройти между наиболее удаленными друг от друга станциями сети, причем в одну сторону проходит неискаженный сигнал, а обратно распространяется уже искаженный коллизией сигнал.

Из-за этого стандарт 802.3 для 10 Мбит/с Ethernet определяет минимальную длину поля данных кадра в 46 байт, что вместе со служебными полями дает минимальную длину кадра 64 байт, а вместе с преамбулой – 72 байт. Отсюда может быть вычислено ограничение на расстояние между станциями. В стандарте для 10 Мбит/с Ethernet время передачи кадра минимальной длины равно 575 битовых интервалов, значит, время двойного оборота должно быть меньше 57,5 мкс. Прибавив межкадровый интервал в 9,6 мкс, получаем, что период следования кадров минимальной длины составляет 67,1 мкс (рис. 2.6).

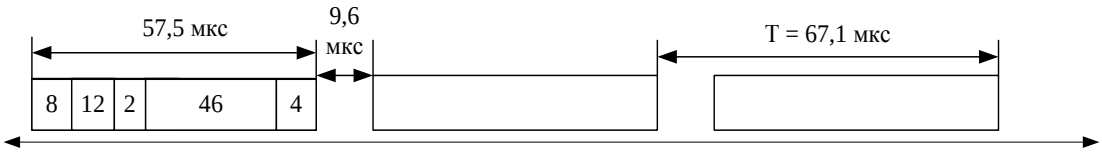


Рис. 2.6. Время передачи кадров Ethernet 10 Мбит/с минимальной длины

В соответствии со стандартом максимальный размер кадра в сети Ethernet 10 Мбит/с составляет 1526 байт (12208 бит), а минимальный — 72 байт (576 бит). При частоте передачи 10 МГц время передачи пакета минимальной длины составляет 57,6 мс. Это время несколько больше, чем удвоенное время распространения сигнала между крайними точками кабеля, равное 51,2 мс. Последняя цифра получена исходя из максимально допустимого в Ethernet расстояния между узлами, равного 2500 м, и зависит от типа кабеля и задержки кадров в повторителях и концентраторах. Так

для стандарта 10Base-5 допускается использование до 4-х повторителей, соединяющих в этом случае 5 сегментов длиной до 500 метров каждый, итого 2500 м.

Максимальное значение скорости устойчивой передачи для метода CSMA/CD определяется в соответствии с соотношением:

$$S = (1+6.2*\tau*C/L) - 1, \qquad (2.6)$$

где: τ — время распространения (включая время приема) в секундах,

C — скорость передачи данных в моноканале,

L — средняя длина кадра.

Как видно из формулы, эффективность метода CSMA/CD определяется длиной моноканала, скоростью передачи данных и минимальной длиной кадра данных.

Параметры метода доступа CSMA/CD для стандарта 10 Мбит/с Ethernet 10base-T приведены в табл. 2.1

Таблица 2.1

Межкадровый интервал	9,6 мкс
Максимальное число попыток передачи	16
Максимальная длина кадра (без преамбулы)	1518 байт
Максимальная длина кадра (без преамбулы)	64 байта
Длина преамбулы	8 байт
Минимальная длина случайной паузы после коллизии	0 битовых интервалов
Максимальная длина случайной паузы после коллизии	524000 битовых интервалов

Домен коллизий

При использовании метода доступа CSMA/CD существует понятие домена коллизий. **Домен коллизий** (collision domain) – это часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части этой сети возникла коллизия. Сеть Ethernet, построенная на общей шине данных, повторителях или концентраторах, всегда образует один домен коллизий. Домен коллизий соответствует одной разделяемой среде. Мосты, коммутаторы и устройства, работающие на сетевом или более высоком уровнях, делят сеть Ethernet на отдельные домены коллизий.

2.3.3. Метод доступа CSMA/CA

Множественный доступ с контролем несущей и избеганием коллизий (Carrier Sense Multiple Access With Collision Avoidance - CSMA/CA) – детерминированный метод доступа к общей среде передачи. Поскольку метод обнаружения коллизий CSMA/CD не может работать в беспроводной сети, то для обнаружения коллизий и потери пакета используется метод CSMA/CA с квитированием – на каждый пакет ожидается подтвер-

ждение доставки, если такой пакет не пришел – значит, произошла коллизия и пакет передается повторно. В настоящее время используется в стандарте беспроводной передачи IEEE 802.11, используя короткие сообщения: запрос на отправку (Request to Send) и готовность к отправке (Clear to Send).

Перед отправкой кадра передающая станция, прослушивает среду передачи, т.е. принимает и анализирует возникающие на нем электрические сигналы. При отсутствии сигнала несущей частоты передающая станция посылает короткий сигнал запроса на передачу (RTS) и определенное время ожидает ответа (CTS) от адресата назначения или координирующего узла, которым в беспроводных сетях является точка доступа. При отсутствии ответа, так как подразумевается возможность коллизии, попытка передачи откладывается, а при получении ответа в общую среду передачи посылается кадр. При запросе на широковещательную передачу, когда RTS содержит широковещательный адрес, сигнал CTS не ожидается.

Более подробно этот метод доступа рассмотрен в разделе, посвященному беспроводным сетям IEEE 802.11.

2.3.4. Метод маркерного доступа

Метод маркерного доступа является детерминированным, в отличие от случайного метода доступа CSMA/CD. Метод маркерного доступа обеспечивает гарантированное время доступа к среде передачи и при высокой загрузке сети гораздо эффективнее случайных методов из-за отсутствия потерь времени из-за коллизии.

Более подробно этот метод доступа рассмотрен в разделе, посвященному сетям Token Ring.

2.4. Форматы кадров Ethernet

Существует несколько форматов Ethernet-кадра.

1. Первоначальный Ethernet Version I (больше не применяется).
2. Ethernet Version 2 или Ethernet II – кадр, ещё называемый DIX (аббревиатура первых букв фирм-разработчиков DEC, Intel, Xerox) – используется по сей день, наиболее широко распространенный формат кадра.
3. Novell – внутренняя модификация IEEE 802.3 без поддержки подуровня LLC.
4. IEEE 802.2 LLC.
5. IEEE 802.2 LLC/SNAP.

Современные компьютерные сети неоднородны по своей природе, а сетевые протоколы используют зачастую разные типы кадров Ethernet. Так, в старых версиях программных средств компании Novell (NetWare 3.x) базовым форматом по умолчанию является формат, соответствующий стан-

дарту IEEE 802.3, а не IEEE 802.2 или IEEE 802.2 с поддержкой протокола доступа к подсети (Subnetwork Access Protocol – SNAP), как это предусмотрено стандартами IEEE (причем, кроме фирмы Novell этот формат больше никто не применял). С выходом NetWare 4.x протоколы IPX/SPX используют по умолчанию стандартные кадры Ethernet, соответствующие IEEE 802.2.

Кадры различных форматов могут сосуществовать в одной сети. Различия в форматах кадров технологии Ethernet могут иногда приводить к несовместимости аппаратуры, рассчитанной на работу только с одним стандартом. Производится автоматическое детектирование типов кадров по характерным значениям некоторых полей.

Например, если значение поля ТП>1500 (0x05DC), то данный кадр - Ethernet II, а значение в этом поле указывает на протокол верхнего уровня.

Если значение поля ТП <1500, то:

если 2 байта (DSAP, SSAP) = 0xFFFF, то кадр - Ethernet 802.3 (устаревшая версия протокола Novell);

если 2 байта (DSAP, SSAP) = 0xAAAA, то кадр - Ethernet SNAP (популярный формат в сетях TCP/IP, более гибкий стандарт, чем Ethernet II);

иначе – это кадр Ethernet 802.2, который использовался фирмой Novell в последних версиях NetWare.

На рис. 2.7 представлены основные форматы кадров Ethernet. Назначение полей кадров имеют следующие значения:

Ethernet II

октеты	7	1	6	6	2	min46, max1500		4
Поле кадра	П	НОК	АП	АО	ТП	Данные	ЗП	КПК

Novell Ethernet 802.3

октеты	8	6	6	2	min46, max1500		4
Поле кадра	П	АП	АО	ДК	Данные	ЗП	КПК

Novell Ethernet 802.2

октеты	8	6	6	2	min46, max1500					4
Поле кадра	П	АП	АО	ТП	ТДСП	ТДСО	У	Данные	ЗП	КПК

Ethernet 802.2 с SNAP

октеты	8	6	6	2	min46, max1500						4
Поле кадра	П	АП	АО	ТП	ТДСП	ТДСО	У	ИП	Дан-ные	ЗП	КПК

П – преамбула (чередование единиц и нулей - 10..10), в Ethernet II восьмой октет преамбулы – начальный ограничитель кадра (**НОК**), имеет вид 10101011.

АП (АО) – адрес получателя (отправителя) имеющий следующий формат:

Для 48 – битового адреса:

И/Г	Г/Л	46 - битовый адрес

Рис. 2.7. Форматы физических адресов Ethernet (MAC адресов)

И/Г = 0 – индивидуальный адрес;

И/Г = 1 – групповой адрес;

Г/Л = 0 – глобально администрируемый адрес;

Г/Л = 1 – локально администрируемый адрес;

АП – адрес получателя (48-бит).

АП, состоящий из одних единиц, т.е. адрес FF-FF-FF-FF-FF-FF, является глобальным или широковещательным (Broadcast).

Адрес групповой рассылки (Multicast) идентифицирует станции, выделенные в отдельную группу получателей администратором сети. Первый бит такого адреса - 1, остальные любые, кроме всех 1. Адрес групповой рассылки не может быть адресом отправителя.

В случае индивидуальных адресов (Unicast) первые три байта служат для идентификации производителя сетевой платы, а последние три байта составляют уникальный номер конкретной платы. Так, первые три байта адреса производителя популярных сетевых плат 3Com соответствуют числу – 02608C в шестнадцатеричной системе счисления. Адрес получателя называется также физическим или MAC-адресом. Он идентифицирует непосредственного получателя на канальном уровне, а не конечного, например, маршрутизатор в сети Ethernet. Конечный получатель идентифицируется с помощью высокоуровневых протоколов. В случае TCP/IP – это IP-адрес станции.

ТП – тип протокола, определяющий высокоуровневый протокол (такой как IP, Apple Talk и т.д.), контейнером для пакета которого служит кадр. В соответствии с принятыми соглашениями, тип протокола задается большим, чем 0x05FE (1518 – максимальная длина кадра). Значения поля типа протокола для некоторых распространенных сетевых протоколов приведены в табл. 2.2.

Таблица 2.2

Internet protocol (IP)	–	0x0800
Address Resolution Protocol (ARP)	–	0x0806
Apple Talk	–	0x809B
Xerox Network System (XNS)	–	0x0600
NetWare IPX/SPX	–	0x8137

ДК – длина поля данных в октетах, если значение поля ДК>1500 (0x05DC), то данный кадр принадлежит к типу Ethernet II, а значение в этом поле указывает на протокол верхнего уровня.

ЗП – заполнитель (если поле данных меньше минимально необходимого, то оно дополняется произвольным набором битов до минимальной длины). Байт заполнения может вставляться, даже если объем передаваемых данных более 46 байт. Так, по предложению фирмы Novell, в случае нечетного количества байт драйвер сетевой платы добавляет еще один. Это сделано

потому, что некоторые старые маршрутизаторы не понимают кадры нечетной длины.

КПК – контрольная последовательность кадра, вычисляется на основе содержимого заголовка и данных (вместе с заполнителем, но без учета преамбулы и ограничителя) с помощью 32-разрядного циклического избыточного кода (CRC) с порождающим полиномом:

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

ТДСП (ТДСО) – однобайтные поля точек доступа к сервису уровня логического управления каналом получателя (отправителя), служащие для определения вышележащего протокола. Как правило, они содержат одно и

ТДСП		ТДСО	
И/Г	Адрес ТДСП	К/О	Адрес ТДСО

И/Г=0 – индивидуальный; **И/Г=1** – групповой**;**

К/О=0 – команда; **К/О=1** – подтверждение**.**

Рис. 2.8. Формат полей ТДСП и ТДСО

то же значение адреса точки доступа и имеют следующую структуру (рис. 2.8):

Адрес ТДСП (Адрес ТДСО) может принимать значения:

0xE0 - для Novell; **0x06** - для TCP/ IP;

0xF0 - для NetBIOS; **AA** - для SNAP.

Поле ТДСП, состоящее из одних единиц, является глобальным и означает группу из всех тех ТДСП, которые активно обслуживаются адресом пункта доступа к услугам нижерасположенного уровня. Поле ТДСП (ТДСО), состоящее из одних нулей, является нулевым адресом и означает тот уровень логического звена, который связан с нижерасположенным адресом пункта доступа к услугам, и не используется для идентификации какого-либо пункта доступа к услугам для сетевого уровня или какого-либо пункта доступа к услугам для соответствующей управляющей функции уровня. Адреса 01000000 и 1100000 рассматриваются как индивидуальный и групповой адреса соответственно для управляющей функции подуровня. Остальные адреса с битами, равными 1 (кроме первого), зарезервированы. В целом назначением номеров точек доступа к сервису занимается IEEE.

У – одно или двухбайтное управляющее поле. Оно обычно задается равным 0x03 и, в соответствии с протоколом LLC, означает, что соединение на уровне звена данных не устанавливается. Значения, которые может принимать данное поле, приведены в табл. 2.3:

Таблица 2.3

	1 байт					2 байт	
I – формат (информационный)	0	N(S)				P/F	N(R)
S – формат (супервизорный)	1	0	S S	X XXX		P/F	N(R)
U – формат (ненумерованный)	1	1	M M	P/F	MMM		

где:

N(S), N(R) – последовательный номер передачи и приема;

P/F – бит запрос / окончание;

S – супервизорный бит;

M – бит модификатора;

X – резервируется, при передаче кодируется нулем.

ИП – дополнительное пятибайтное поле для идентификации протокола, причем значения двух последних байтов этого поля совпадают со значениями поля протокола в Ethernet II (например, 0x8137 для NetWare). Это поле протокола доступа подсети (SNAP) было разработано с целью увеличения числа поддерживаемых протоколов, так как однобайтные поля ТДСП (ТДСО) поддерживают не более 256 протоколов.

2.5. Структурированные кабельные системы

Структурированная кабельная система (Structured Cabling System, SCS) — это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях. Кабельная система является фундаментом любой сети, поэтому к ней предъявляются высокие требования, ответом на которые стали структурированные кабельные системы.

Структурированная кабельная система представляет своего рода «конструктор», с помощью которого проектировщик сети строит нужную ему конфигурацию из стандартных кабелей, соединенных стандартными

разъемами и коммутируемых на стандартных кроссовых панелях. При необходимости конфигурацию связей можно легко изменить — добавить сегмент, коммутатор, изъять ненужное оборудование, а также поменять соединения между сетевым оборудованием и оконечными станциями.

При построении структурированной кабельной системы подразумевается, что каждое рабочее место на предприятии должно быть оснащено розетками для подключения телефона и компьютера, даже если в данный момент этого не требуется. Т.е. хорошая структурированная кабельная система строится избыточной. В будущем это может сэкономить средства, так как изменения в подключении новых устройств можно производить за счет перекоммутации уже проложенных кабелей.

Структурированная кабельная система планируется и строится иерархически, с главной магистралью и многочисленными ответвлениями от нее (рис. 2.9).

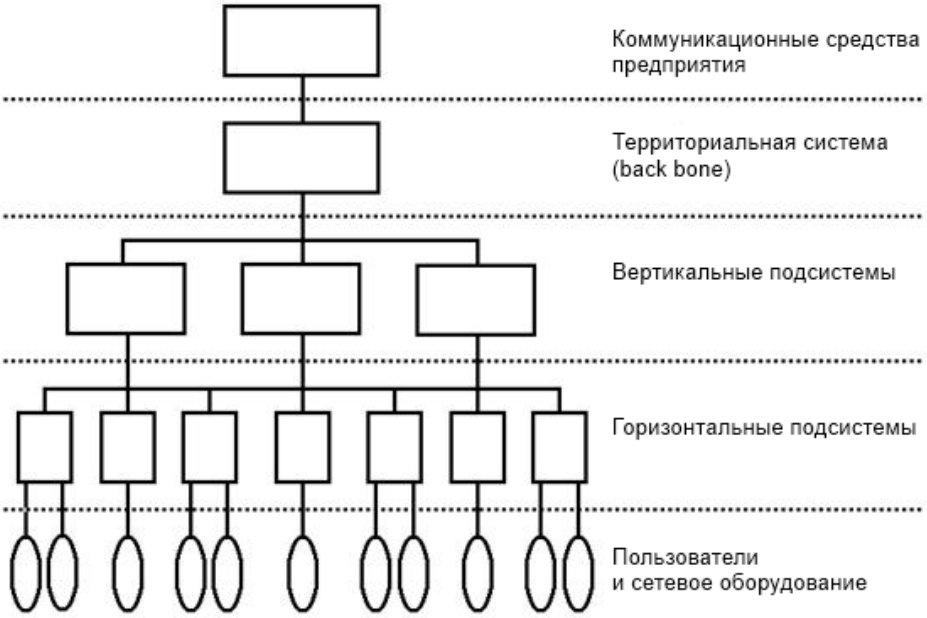


Рис. 2.9. Структурированная кабельная система

Типичная иерархическая структура структурированной кабельной системы (рис. 2.10) включает:

- территориальную (магистральную) систему;
- горизонтальные подсистемы (в пределах этажа);
- вертикальные подсистемы (для связи между этажами).

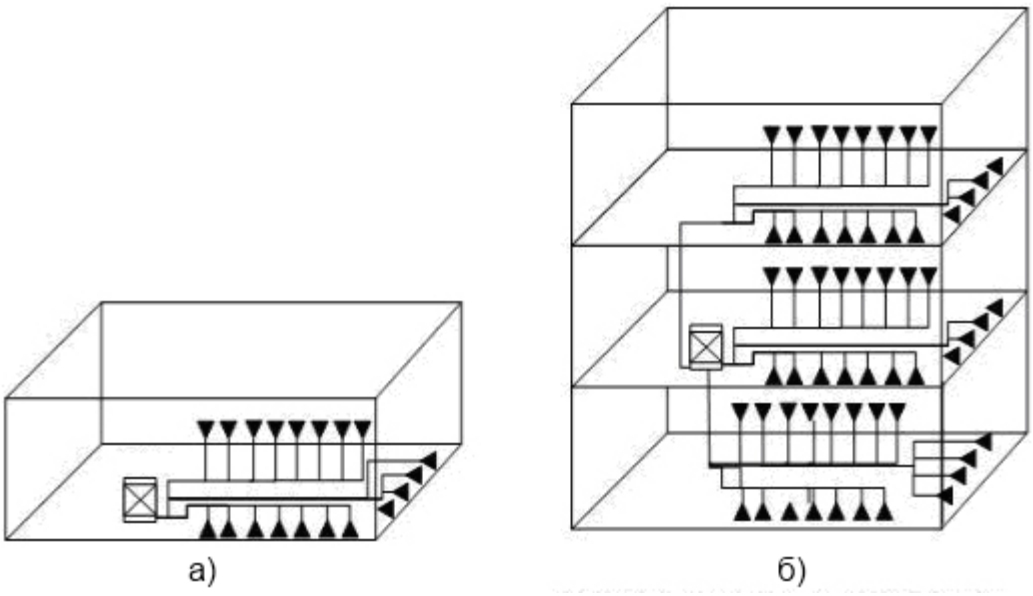


Рис. 2.10. Горизонтальная (а) и вертикальная (б) структурированная кабельная системы

Горизонтальная подсистема соединяет кросс (кроссовый шкаф) этажа с розетками для подключения пользователей и оборудования. Подсистемы этого типа соответствуют этажам здания. Для горизонтальной подсистемы характерно наличие большого количества ответвлений и перекрестных связей. Наиболее распространенный для нее тип кабеля — неэкранированная витая пара категории 5 или 6.

Вертикальная подсистема соединяет кроссы (кроссовые шкафы) каждого этажа с центральной аппаратной здания. Вертикальная подсистема состоит из более протяженных отрезков кабеля, количество ответвлений намного меньше, чем в горизонтальной подсистеме. Предпочтительный для нее тип кабеля — волоконно-оптический.

Использование структурированной кабельной системы вместо хаотически проложенных кабелей дает предприятию много преимуществ:

Универсальность. Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы контроля, мониторинга и управления хозяйственными службами и системами жизнеобеспечения предприятия.

Увеличение срока службы. Срок морального старения хорошо структурированной кабельной системы может составлять до 10 лет.

Уменьшение стоимости добавления новых пользователей и изменения мест размещения сетевого оборудования. Известно, что стоимость кабельной системы значительна и определяется в основном не стоимостью

кабеля, а стоимостью работ по его прокладке. Предусматривается запас кабеля по длине, чтобы несколько раз не выполнять прокладку, наращивая длину кабеля. При таком подходе все работы по добавлению или перемещению оборудования сводятся к его подключению к уже имеющейся розетке.

Возможность легкого расширения сети. Структурированная кабельная система является модульной, поэтому ее легко расширять. Например, к магистрали можно добавить новую подсеть, не оказывая никакого влияния на существующие подсети. Можно заменить в отдельной подсети тип кабеля независимо от остальной части сети. Структурированная кабельная система является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты.

Обеспечение более эффективного обслуживания. Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой. При шинной организации кабельной системы отказ одного из устройств или соединительных элементов приводит к трудно локализуемому отказу всей сети.

2.6. Физическая среда передачи данных. Проводная среда

В качестве проводной среды передачи данных используются различные виды кабелей: коаксиальный кабель, кабель на основе экранированной и неэкранированной витой пары и оптоволоконный кабель. Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) в настоящее время является неэкранированная витая пара.

Кабели на основе витых пар делятся на **экранированные** (Shielded twisted pair - STP) и **неэкранированные** (Unshielded twisted pair - UTP). Эти кабели имеют 2 отличия. Первое: в UTP используют 4 пары проводников, а в STP - две. Второе, и основное отличие заложено в самом названии. В STP предусмотрен дополнительный проводящий слой, окружающий витые провода, который обеспечивает дополнительную защиту от помех. В то же время дополнительный слой придаёт кабелю жёсткость. Кроме того, такая защита эффективна только при правильном заземлении и целостности экранизирующего слоя. В кабеле UTP использован другой подход к проблеме защиты от электромагнитных помех. В кабеле UTP, где два провода скручены друг с другом, каждый в отдельности провод является приемником шума, но эти шумы противофазные, тогда как помеха синфазна, и во вторичные обмотки приемника сигнал шума U_n не передается, потому как на выходном трансформаторе гальванической развязки напряжение на обмотке равно U_c (рис. 2.11).

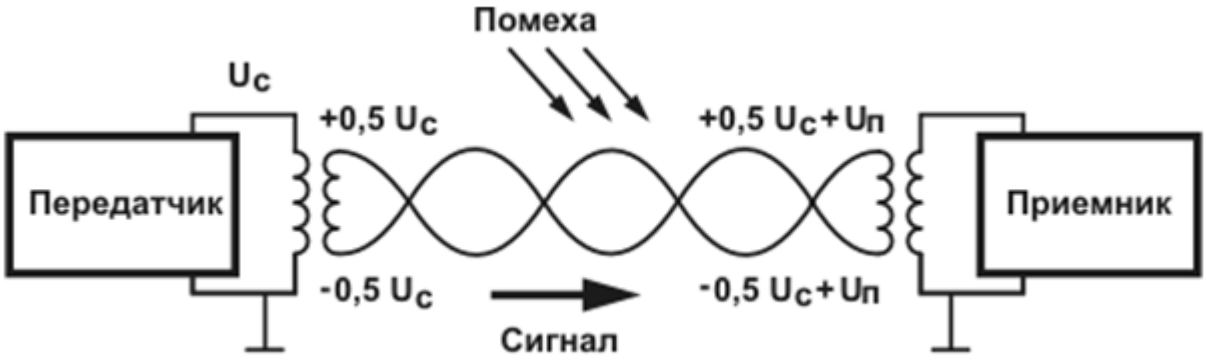


Рис. 2.11. Механизм работы защиты от электромагнитных помех

Однако следует учитывать, что гальваническая развязка токовой петлей не подразумевает передачу постоянной составляющей сигнала.

В зависимости от механических и электромеханических параметров UTP делятся на 7 категорий, которые нумеруются от CAT1 до CAT7 (от category или категория, сокращение «CAT») и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов, и каждая пара имеет больше витков на единицу длины. Таким образом, хотя и не существует кабелей, которые совершенно не чувствительны к помехам, чем выше категория кабеля UTP, тем менее он подвержен помехам и, соответственно, обеспечивает более быструю и точную передачу данных. Категории экранированной и неэкранированной витой пары описываются в стандарте EIA/TIA 568 (Американский стандарт проводки в коммерческих зданиях) и в международном стандарте ISO 11801, а также в ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008 (де факто являющимся переводом EIA/TIA 568).

Кабели категории 1 применяются там, где требования к скорости передачи минимальны. Обычно это кабель для цифровой и аналоговой передачи голоса и низкоскоростной (до 20 Кбит/с) передачи данных в сетях ТФОП.

Кабели категории 2 применяются для передачи сигналов со спектром до 1 МГц.

Кабели категории 3 обеспечивают передачу данных со скоростью до 10 Мбит/с и содержат не менее 3-х скруток не погонный фут (0,3048 м).

Кабели категории 4 представляют собой улучшенной вариант кабелей категории 3, предназначены для передачи сигналов со спектром до 20 МГц. На практике используются редко.

Кабели категории 5 были специально разработаны для поддержки высокоскоростных протоколов. Кабели допускают скорость передачи до 100 Мбит/с и позволяют расположить сетевое оборудование на расстоянии до 90 м. Большинство высокоскоростных стандартов ориентируются на использование UTP 5 категории. На этом кабеле работают протоколы со скоростью передачи данных 100 Мбит/с – FDDI, Fast Ethernet, 100 VG – Any

LAN, а также более скоростные протоколы – ATM со скоростью 155 Мбит/с и Gigabit Ethernet на скорости 1000 Мбит/с, при использовании четырехпарного кабеля.

Кабель улучшенной категории 5 (UTP CAT 5e/CIass D) несколько усовершенствован по сравнению с кабелем категории 5: форма витков намного разнообразнее, в нём использованы провода повышенного качества, и он соответствует стандарту Ethernet 1000 Base-T.

Для кабелей категории 6 частотные характеристики определяются до 250 МГц, для кабеля категории 7 – до 600 МГц. Спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, скорость передачи данных для кабелей категории 7 до 10 Гбит/с.

Кабели категории 7а (полоса частот до 1200 МГц) разработаны для передачи данных на скоростях до 40 Гбит/с на расстояние до 50 м или до 100 Гбит/с на расстояние до 15 м.

Согласно стандарту ISO 11801 кабели STP подразделяются по функциональным признакам, а не по степени устойчивости к радиочастотным помехам.

Тип 1. Одножильный кабель STP, используемый для передачи данных. Каждый кабель состоит из 2-х пар проводов.

Тип 2. Сочетание 4-х неэкранированных и 2-х экранированных одножильных проводов в единой оболочке. UTP предназначены для передачи речевых сообщений, а STP – для передачи данных.

Тип 3. Состоит из 4-х пар одножильных проводов, используемых для передачи речевых сообщений и данных.

Тип 6. Состоит из 2-х пар многожильных кабелей. Во многом подобен типу 1, однако вместо одножильного используется многожильный провод.

Тип 8. Специальный плоский кабель STP, что позволяет прокладывать его под тонкими покрытиями (коврами, линолеумом).

Тип 9. Состоит из 2-х экранированных пар STP, покрытых специальной оболочкой (полиэтиленом), а не поливинилхлоридном (ПВХ), поэтому его можно прокладывать в перекрытиях между этажами здания. При горении ПВХ выделяет токсичные газы, поэтому в соответствии с правилами пожарной безопасности использовать его запрещено.

Для соединения витой пары с сетевыми адаптерами используются восьми контактные разъемы RJ-45 (рис. 2.12).

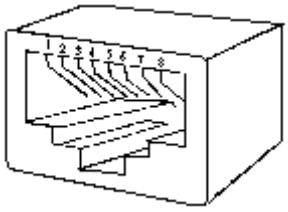


Рис. 2.12. Разъем RJ-45

В табл. 2.4 приведены сигналы, соответствующие номерам контактов разъема RJ-45 для передачи Ethernet 100Base-TX.

Таблица 2.4

Тип	Каскадирование	Нормальный режим
1	RD+ (прием)	TD+ (передача)
2	RD- (прием)	TD- (передача)
3	TD+ (передача)	RD+ (прием)
4	Не используется	Не используется
5	Не используется	Не используется
6	TD- (передача)	RD- (прием)
7	Не используется	Не используется
8	Не используется	Не используется

Рассмотрим количественные параметры кабелей на витой паре.

Погонное затухание (attenuation) - потеря мощности сигнала, выражаемая в децибелах (дБ, dB):

$$dB=10*\log_{10}(P_{вх}/P_{вых}) \qquad (2.7)$$

Затухание в кабеле зависит от таких факторов, как размер и состав проводника (медь, алюминий), материала изоляции, рабочей частоты (диапазона частот) и длины кабеля.

Переходное затухание (перекрестные помехи) характеризует помехи от активного сигнала, наведенные в соседней витой паре; выражается в децибелах (дБ, dB):

$$dB=20*\log_{10}(U_{вх}/U_{наведен.}) \qquad (2.8)$$

Переходное затухание на ближнем конце (NEXT, Near End Cross Talks). Сигнал имеет наибольшую мощность сразу же после момента передачи данных, поэтому именно на ближнем конце он производит наибольшие наводки в соседней витой паре.

Суммарное переходное затухание (PS NEXT, Power Sum NEXT). Некоторые сетевые архитектуры задействуют сразу несколько пар при передаче в одном направлении, поэтому PS NEXT важно контролировать после прокладки СКС.

Переходное затухание на дальнем конце (FEXT, Far End Cross Talks). Также этот параметр актуален для систем, использующих одновременно несколько витых пар при передаче, например, в Gigabit Ethernet. FEXT характеризует последствия полнодуплексных операций, когда сигналы генерируются одновременно на ближнем и дальнем концах. Для его измерения с одной стороны кабеля генерируют сигнал в линию, с другой на неактивной паре измеряют напряжение наведенного сигнала.

Возвратные помехи (Return Loss). Любое отклонение от импеданса кабельной сети по длине кабеля приведет к тому, что часть сигнала отразится назад к источнику данных (т.е. уменьшится энергия сигнала в прямом направлении). Изменение импеданса может быть вызвано множеством причин:

- несоблюдением технологии в процессе изготовления (расстояние между проводниками, нарушение свойств изолирующего материала);
- несоответствием компонентов (кабель 5 категории, розетка - для 3 категории);
- неправильная укладка СКС (несоблюдение норм на радиус изгиба, монтажа разъемов на кабель).

Таблица 2.5

Сравнительные показатели UTP

Частота [МГц]	**Cat. 3**		**Cat. 5**		**Cat. 5e**		**Cat. 6**		**Cat. 7**	
	Att. [dB]	NEXT [dB]	Att. [dB]	NEXT [dB]	Att. [dB]	NEXT [dB]	Att. [dB]	NEXT [dB]	Att. [dB]	NEXT [dB]
1	2.6	41.0	2.1	62.0	2.1	65.0	2.1	66.0	2.1	80.0
4	5.6	32.0	4.3	53.0	4.3	56.0	3.8	66.0	3.9	80.0
10	9.7	26.0	6.6	47.0	6.6	50.0	6.0	60.0	6.0	80.0
20			9.2	42.0	9.2	45.0	8.5	55.5	8.5	80.0
62,5			17.1	35.0	17.1	38.0	15.5	48.1	15.0	75.0
100			22.0	32.0	22.0	35.0	19.9	45.0	19.0	71.0
155							25.3	42.2	24.0	68.0
200							29.2	40.5	27.0	66.0
300									33.0	64.0
600									50.0	60.0

где: Att. (attenuation) - погонное затухание
NEXT - переходное затухание на ближнем конце

Коаксиальный кабель (от лат. co – совместно и axis – ось, то есть «соосный») – электрический кабель, состоящий из расположенных соосно центрального проводника и экрана. Изобретён и запатентован в 1880 году британским физиком Оливером Хевисайдом. Обычно служит для передачи высокочастотных сигналов, для которых позволяет осуществить большую защиту от электромагнитных помех и более низкое затухание, чем витая пара.

Первые локальные сети появились при финансировании министерства обороны США, поэтому типы коаксиальных кабелей для Ethernet 10 Мб регламентировал военный стандарт США MIL-C-17, согласно нему основными типы и характеристиками коаксиальных кабелей, использовавшихся в локальных КСПД, являются:

- RG – 8 и RG – 11 – «толстый» коаксиальный кабель, разработанный для первых сетей Ethernet 10Base-5. Имеет волновое сопротивление 50 Ом и внешний диаметр около 12 мм. Внутри находится достаточно толстый проводник – 2,17 мм. Из-за своего диаметра и диаметра проводника этот кабель было сложно монтировать, т.к. он очень жёсткий, кроме того, при присоединении к сетевому адаптеру возникали некоторые сложности — использовались трансиверы (Attachment Unit Interface - AUI), присоединённые к сетевой карте с помощью ответвления, пронизывающего кабель, иногда называемые «вампирчики». За счёт более толстого проводника, и соответственно низкого затухания, передачу данных можно было осуществлять на расстояние до 500 м со скоростью 10 Мбит/с.
- RG – 58/U, RG – 58 A/U и RG – 58 C/U – виды «тонкого» коаксиального кабеля для сетей Ethernet 10Base-2, наша промышленность согласно ГОСТ 11326.0-78 выпускает аналогичный кабель РК-50. Кабель RG – 58/U имеет сплошной внутренний проводник, а RG – 58 A/U – многожильный. Все эти разновидности кабеля имеют волновое сопротивление 50 Ом. Тонкий внутренний проводник 0,89 обладает гораздо большей гибкостью, что удобно при монтаже. Стоимость сетевого оборудования, необходимого для создания сети на «тонком» кабеле, относительно невелика.

Чтобы сделать кабель совершенно нечувствительным к электромагнитному излучению, можно использовать **оптоволоконные кабели**, в которых для передачи данных применяют световые, а не электрические импульсы.

Основа оптоволокна – оксид кремния (кварц), самый распространенный в природе материал, недорогой в отличие от меди, однако для дальнего инфракрасного диапазона могут использоваться другие материалы, такие как фторцирконат, фторалюминат и халькогенидные стекла. В настоящее время развивается применение пластиковых оптических волокон. Сер-

дечник в таком волокне изготовляют из полиметилметакрилата (PMMA), а оболочку из фторированных PMMA (фторполимеров).

Оптическое волокно, обычно, имеет круглое сечение и состоит из двух частей — сердцевины и оболочки, оптические волокна (сердцевина) могут иметь диаметр менее 100 микрон, малый вес и могут применяться в авиации, приборостроении, кабельной технике. Оптические волокна, используемые в КСПД, как правило, имеют диаметр 125 микрон.

Оптоволоконные кабели бывают двух типов: одномодовые и многомодовые (рис. 2.13). Одномодовый кабель передаёт данные по единственному тракту. Центральный проводник в таком кабеле имеет диаметр, соизмеримый с длиной волны света, от 5 до 10 мкм. Поэтому луч света распространяется вдоль оси световода, не отражаясь от внешнего проводника, за счёт чего исключается влияние дисперсионных искажений и луч имеет высокую интенсивность.

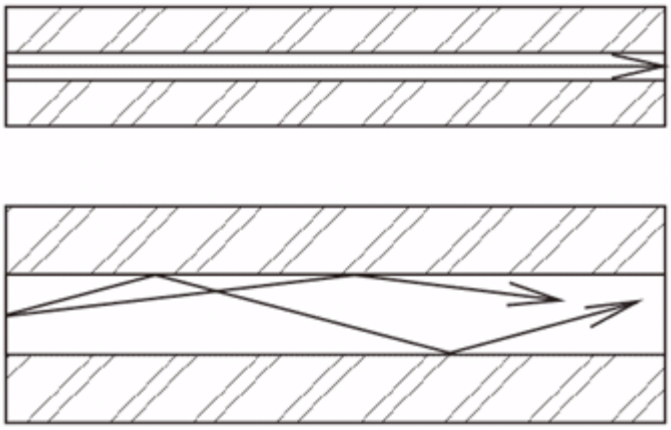


Рис. 2.13. Одномодовое (выше) и многомодовое (ниже) оптоволокно

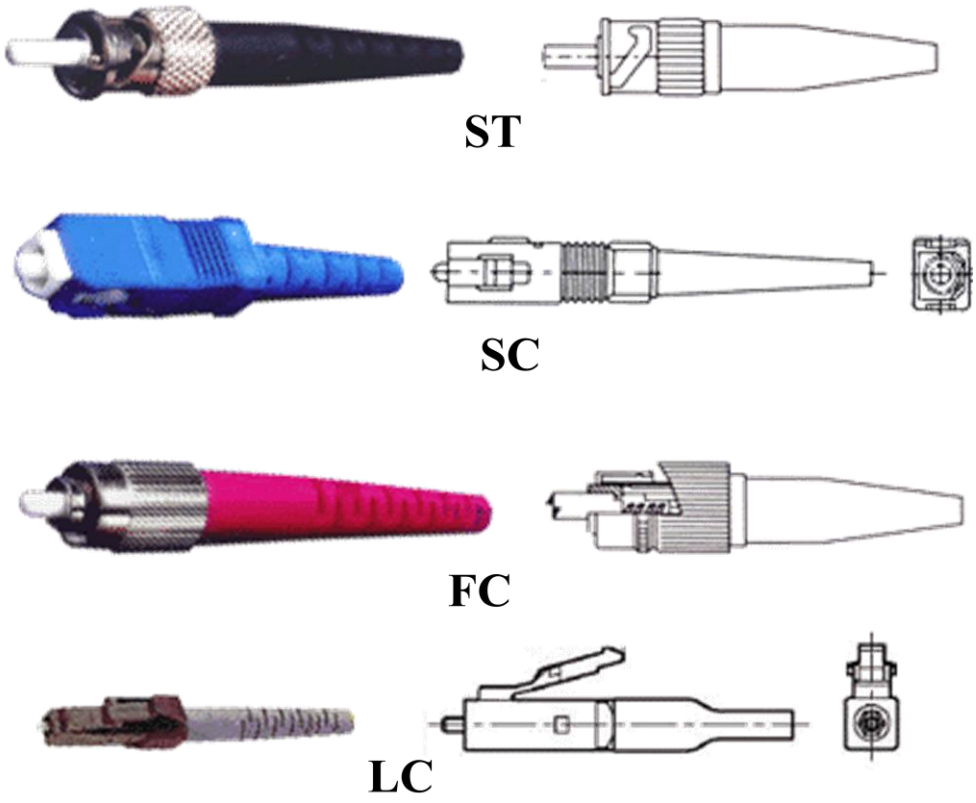


Рис. 2.14. Оптические коннекторы

В многоводных кабелях используются более широкие внутренние сердечники, диаметр которых составляет 50 микрон в европейском стандарте и 62,5 микрон в североамериканском, поэтому их легче изготовить технологически. При распространении света в таких кабелях существует одновременно несколько лучей, отражающихся от внешнего проводника под разными углами, что приводит к модальной дисперсии, т.е. рассеянию исходного импульса, его форма из прямоугольного превращается в колоколоподобную. Модальная дисперсия приводит к сужению полосы пропускания.

Стоимость оптоволоконного кабеля не сильно превышает стоимость кабелей на витой паре, но монтажные работы с оптоволокном обходятся намного дороже из-за трудоёмкости операций и высокой стоимости применяемого монтажного оборудования.

В России при монтаже волоконно-оптических сетей используют виды разъемов, представленные на рис. 2.14.

Оптический разъем типа ST соответствует международному стандарту IEC 874-10 и имеет наконечник диаметром 2,5 мм с выпуклой торцевой поверхностью. Фиксация вилки на розетке выполняется подпружиненным байонетным элементом. Металлическое исполнение корпуса вилки и розетки разъема ST обеспечивает высокую механическую прочность в сочетании с простотой монтажа и подключения.

Коннектор типа SC имеет пластмассовый корпус, хорошо защищающий наконечник, и обеспечивает плавное подключение одним линейным движением. Наконечник разъема SC утоплен в корпус вилки, что предохраняет его от загрязнений. Линейное движение при подключении и отключении делает этот разъем удобным для применения в 19-дюймовых кроссах, и позволяет увеличить плотность расположения портов.

Разъемы SC обеспечивают большую стабильность параметров (не менее 500 подключений и отключений), чему способствует отсутствие проворачиваний наконечников относительно друг друга при включениях и отключениях.

Разъемы типа FC ориентированы на применение в одномодовой технике. Конструкция разъема обеспечивает надежную защиту керамического наконечника от загрязнений, а применение для фиксации накидной гайки дает большую герметичность зоны соединения и надежность соединения при воздействии вибраций.

Розетки разъема FC выпускаются в двух вариантах: с квадратным фланцем и креплением двумя винтами и с круглым фланцем и креплением под гайку.

Коннектор типа LC имеет прочный термостойкий пластмассовый корпус типа push-pull, с подпружиненным керамическим наконечником диаметром 1,25 мм. Коннектор фиксируется в розетке защелкой аналогично коннекторам для витой пары RJ-типа. Коннекторы могут соединяться в дуплексную пару с помощью специального зажима. Небольшие размеры коннекторов обеспечивают стабильность их взаимного расположения в розетке. Линейное движение при подключении и отключении делает этот разъем удобным для применения в 19-дюймовых кроссах.

2.6.1. Технологии FTTx

В настоящее время уже есть целая концепция абонентских кабельных сетей нового поколения. Связана она с семейством концепций **FTTx (**fiber to the x — оптическое волокно до точки x), соответственно, вместо x добавляются различные варианты доведения оптического транспорта к пользователю (рис. 2.15):

- FTTB (fiber to the building) - оптическая система передачи к дому;
- FTTN / FTTC (fiber to the node) - оптическая система передачи до узла;
- FTTO (fiber to the office) - оптическая система передачи в офис;
- FTTH (fiber tothe home) - оптическая система передачи в квартиры.

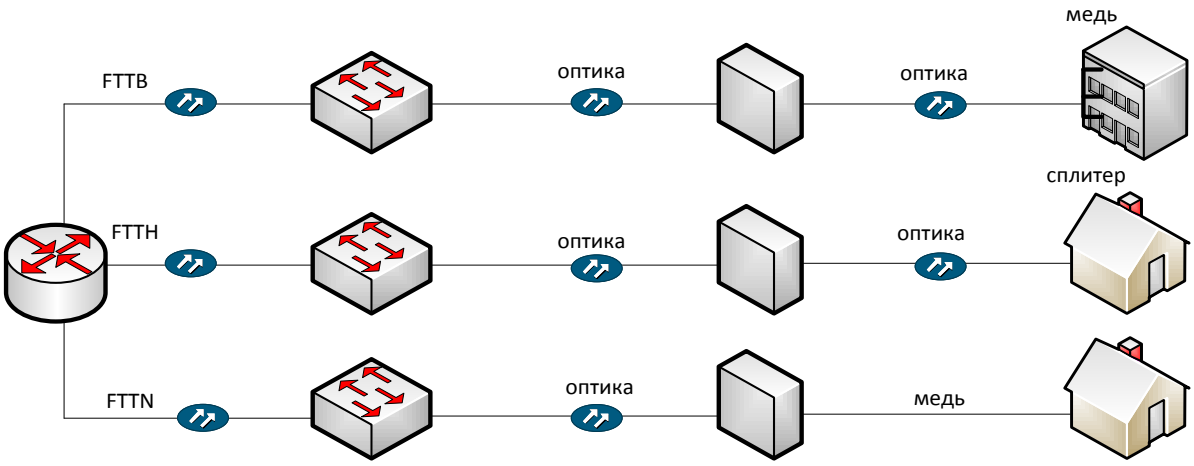


Рис. 2.15. Варианты построения сетей FTTx

Широкая полоса систем FTTx открывает новые возможности предоставления абонентам большего числа услуг. В табл. 2.6 приведено сравнение технологии доступа.

Таблица 2.6

Сравнение технологий доступа

Технология	Пропускная способность (к абоненту - от абонента)	Максимальная протяженность	Дополнительное промежуточное оборудование
ADSL2 +	24Мбит/с - 3 Мбит/с	2,4 км (медная пара)	нет
VDSL2	24Мбит/с – 3 Мбит/с	2,4 км (медная пара)	нет
GePON	2,4 Гбит/с – 1,25 Гбит/с	20 км (оптоволокно) + (сплиттер)	Сплиттер
P2P/AE	1 Гбит/с - 1 Гбит/с	80 км (оптоволокно)	Нет
FTTB + VDSL2	100 Мбит/с – 50 Мбит/с	20 км (оптоволокно) +0,5 км	Удаленный IP DSLAM-мультиплексор
FTTN + VDSL2	100 Мбит/с – 50 Мбит/с	20 км (оптоволокно) +0,5 км	В защитном исполнении

Сегодня наиболее популярны три группы технологий: пассивных оптических сетей (Passive optical network – PON), Ethernet (в коммутируемом варианте) и гибридных коаксиально-оптических сетях (Hybrid fiber-coaxial

– HFC), при использовании сетей, построенных для кабельного телевидения.

Технология FTTB - волокно до дома, когда к каждому зданию подходит оптико-волоконный канал, что обеспечивает полную защищенность передаваемого сигнала от электромагнитных и радиочастотных помех, дает возможность предоставить высокие скорости доступа. Это наиболее востребована сегодня технология строительства новых широкополосных сетей. Причина этому - снижение за последние годы цены на оптический кабель, появление дешевых оптических приемников, передатчиков. Использование оптики в FTTB позволяет использовать для передачи данных технологию Metro Ethernet, которая по сравнению со стандартом передачи данных по коаксиальному (телевизионному) кабелю (Data Over Cable Service Interface Specifications – DOCSIS) приносит ощутимое увеличение в скорости передачи данных.

Ethernet-коммутатор или DSLAM-мультиплексор в здании подключается к точке присутствия с использованием одного или пары оптических волокон (активный Ethernet). Агрегированный трафик здания передается через это соединение с использованием стандарта Gigabit Ethernet или 10 Gigabit Ethernet. Соединения между абонентами и коммутатором здания могут осуществляться с использованием витой пары, на базе одного из механизмов Ethernet-транспорта в зависимости от среды передачи для вертикальных каналов.

FTTH - это технология прокладки волокна в дом. Учитывая, что абоненты проживают в основном в многоквартирных домах, FTTH означает, в отличие от FTTB, доведение оптического волокна до квартиры абонента.

FTTH реализуется, как правило, в двух конфигурациях оптоволоконных подключения: пассивные оптические сети (PON) и традиционная технология активных оптических сетей Ethernet «точка-точка». Каждый из терминалов оптической сети (ONT) в помещении абонента подключается отдельной жилой к порту коммутатора в точке присутствия или к оптическому сплиттеру, от которого до точки присутствия прокладывается общая оптоволоконная линия. В случае подключения по схеме «точка-точка» применяются стандарты передачи 100BASE-LX или 1000BASE-LX.

Большие затраты на FTTH связаны как со стоимостью оборудования, так и с ценой монтажа. В технологии FTTB преобразователи (оптический узел и медиа конвертеры) устанавливаются в расчетах на каждый дом (60-300 квартир), а при FTTH - каждому абоненту. При использовании PON кроме этого оборудования каждому абоненту нужно установить еще и сплиттеры. Нужно отметить также рост числа необходимых оптических волокон и разветвителей. Более высокая стоимость монтажа объясняется также и большим количеством устанавливаемых оптических кроссов. Если при FTTB они обычно устанавливаются один на здание, то при FTTH – один на каждый этаж. Сравнение технологий FTTx приведено в табл. 2.7.

Таблица 2.7

Сравнение технологий FTTB и FTTH

FTTB		FTTH	
Достоинства	Недостатки	Достоинства	Недостатки
1. Простая и традиционная архитектура сети. 2. Простота установки и ремонта домовой проводки на основе кабеля 5 категории. 3. Абонентский терминал необходим только тем абонентам, которые будут использовать IPTV. 4. Гибкое развитие сети с использованием функционала оборудования.	1. Присутствие большого количества активных устройств в распределительной сети. 2. Осложнение и подорожание эксплуатации сети. 3. Склонность медной домовой проводки к электромагнитным помехам. 4. Сложная архитектура в разветвленных сетях 5. Проблемы с активным оборудованием в распределительной сети (нестабильность электропитания, повреждения, вандализм).	1. Полностью пассивная распределительная сеть. Единая и стабильная среда передачи - оптика. 2. Полное управление сетью из одной точки. Упрощение и снижение стоимости процессов эксплуатации (до 50%). 3. Снижение энергопотребления (до 70%) и арендной стоимости (до 50%). 4. Ориентир на будущее. Высокие скорости и огромный потенциал роста. Сеть и абонентские устройства уже готовы к оказанию множества услуг. 5. Возможность развития сети различных топологий FTTH, B с одного узла.	1. Необходимость установки ONT у каждого абонента. 2. Работа телефона зависит от питания на ONT. 3. Возможна недостаточная квалификация персонала для работы с FTTH решениями.

FTTN (C) - оптические каналы проложены до мультисервисного узла доступа (разделительного узла), к абоненту идут DSL-каналы.

Сохранение участка медного кабеля в смешанной медно-оптической среде доступа объясняется еще и тем, что замена медного кабеля оптическим на последних нескольких сотнях метров абонентской линии требует больших затрат, поскольку, во-первых, последний участок является индивидуальным для каждого абонента и, во-вторых, необходима полная замена абонентской проводки в помещении каждого пользователя.

Коммутатор или DSLAM-мультиплексор в уличном коммутационном шкафу подключается к точке присутствия с использованием одного или пары оптических волокон. Агрегатный трафик от окружающих абонентов передается через это соединение с использованием стандарта Gigabit

Ethernet или 10 Gigabit Ethernet. Сообщение между абонентами и коммутатором в уличном шкафу может осуществляться с использованием оптоволокна (активная оптическая сеть) с пропускной способности 100 Мбит/с или 1000 Мбит/с, или по витой паре с использованием технологии VDSL2.

Исходя из сравнения технологий FTTx, обычно технология FTTB используется для многоэтажной застройки, так как она является наиболее экономически выгодным для густонаселенных районов. Для частного сектора обычно используется технология FTTN (C), которая является наиболее выгодной для частного сектора. Где же необходима высокая надежность и гарантированная полоса для передачи данных, используется технология FTTH. На рис. 2.16 приведены варианты построения сети доступа для разных категорий пользователей.

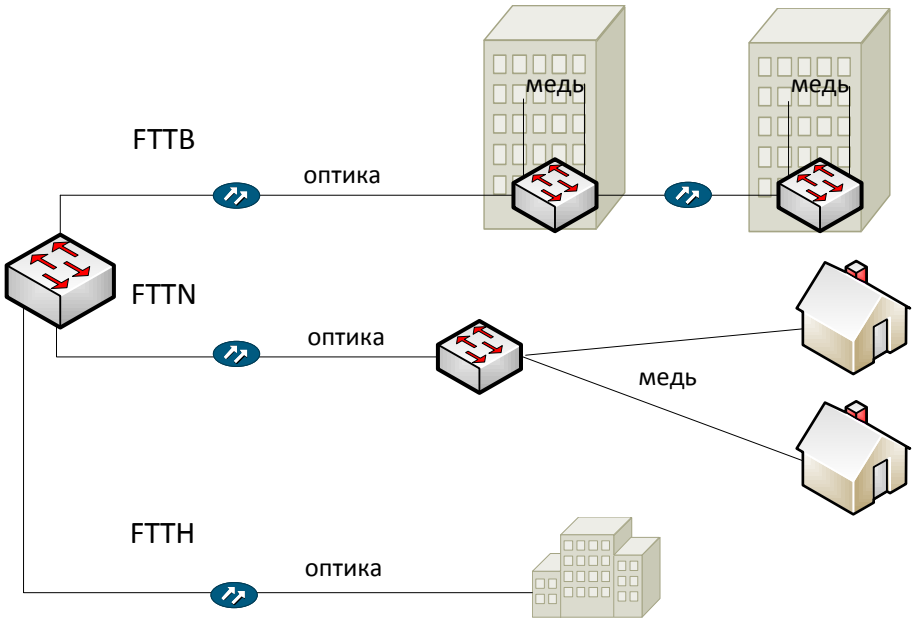


Рис. 2.16. Варианты построения сети доступа

2.7. Физическая среда передачи данных. Типы сетей Ethernet

В рамках развития архитектуры протоколов IEEE определил деление физического уровня на три подуровня:

– передачи физических сигналов (Physsical Signalling – PS);
– интерфейса с устройством доступа (Access-Unit Interface - AUI);
– интерфейса подключения к физической среде (Physical Medium Attachment - PMA).

Подуровень PS выделяется в целях облегчения технического сопряжения с уровнем звена данных. Подуровень PMA согласует сигналы, поступающие из подуровня PS, с требованиями передающей среды, обеспечивая тем самым возможность использования одного PS с несколькими типами передающей среды. Подуровень AUI определяет параметры интер-

фейса между подуровнями PS и PMA (параметры физического соединителя – кабеля, объединяющего подключаемое устройство, реализующее уровень PS, и средства подключения к физической среде, реализующие подуровень PMA).

Стандарт Ethernet (IEEE 802.3) определяет несколько стандартов физического уровня, отличающихся типом используемого кабеля, длиной сегмента, типом коннекторов и скоростью передачи пакетов (табл. 2.8).

Таблица 2.8

Стандарт	Битовая скорость (Мбод)	Тип кабеля	Длина сегмента	Тип коннектора	Канальное кодирование
10Base-5	10	«Толстый» коаксиал (RG-11)	500	AUI	Манчестер-II
10Base-2	10	«Тонкий» коаксиал (RG-58)	185	BNC	Манчестер-II
10Base-T	10	Две неэкранированные витые пары категории 5	100	RJ-45	Манчестер-II
10Base-F	10	Волоконно-оптический кабель	2000	ST и др.	Манчестер-II
100Base-TX	125	Две экранированные или неэкранированные витые пары категории 5	100	RJ-45	4B/5B, MLT-3
100Base-T4	33	Четыре неэкранированные витые пары категории выше 2	100	RJ-45	8B/6T
100Base-FX	125	Волоконно-оптический кабель	2000	ST и др.	4B/5B, NRZI
1000Base-T	1000	Четыре экранированные или неэкранированные витые пары категории 6	100	RJ-45	PAM5
1000Base-LX	1250	Волоконно-оптический кабель одномодовый 1310 nm	5000	LC и др.	8B/10B
1000Base-SX	1250	Волоконно-оптический кабель 860 нм	220	LC и др.	8B/10B
1000Base-EX	1250	Волоконно-оптический кабель одномодовый 1310 nm	40000	LC и др.	8B/10B
10GBase-SR	10000	Волоконно-оптический кабель 850 нм	400	LC и др.	64B/66B
10GBase-ER	10000	Волоконно-оптический кабель 850 нм	40000	LC и др.	64B/66B
10GBase-LX4	12500	Волоконно-оптический кабель 1310 нм	10000	LC и др.	8B/10B
10GBase-LR	10000	Волоконно-оптический кабель	10000	LC и др.	64B/66B
10GBase-T	10000	Четыре экранированные или неэкранированные витые пары категории 7	100	RJ-45	128 QAM

Стандарты 10Base-2 и 10Base-5 определяют сеть Ethernet со скоростью 10 Мбит/с, строящуюся на базе «тонкого» (RG-58) и «толстого» (RG-11) коаксиального кабеля. Предельные расстояния для толстого коаксиаль-

ного кабеля с сопротивлением 50 Ом («толстый» «Ethernet») - 500 м, для тонкого коаксиального кабеля («тонкий» «Ethernet») - 185 м.

Когда устройству в такой Ethernet-сети необходимо переслать кадры другому устройству, оно генерирует в коаксиальном кабеле сигнал, который доставляется ко всем устройствам, подключенным к шине. На рис. 2.17 показан основной принцип работы Ethernet-сети стандарта 10Base2, в которой используется общая электрическая шина, созданная с использованием коаксиального кабеля.

Рис. 2.17. Фрагмент 10Base2 сети

Для стандартов 10Base-5 и 10Base-2 сеть имеет топологию, называемую «общая шина» – все компьютеры подключаются к общему отрезку коаксиального кабеля, оба конца которого «заглушены» согласующими сопротивлениями (50 ом) – **терминаторами** (рис. 2.18). Такой отрезок носит название **сегмента**. Один сегмент сети может включать до 100 рабочих станций, а несколько таких сегментов можно соединять повторителями. В целом, в одной такой сети Ethernet может работать до 1024 рабочих станций, при этом на пути между любыми двумя станциями может стоять максимум два повторителя.

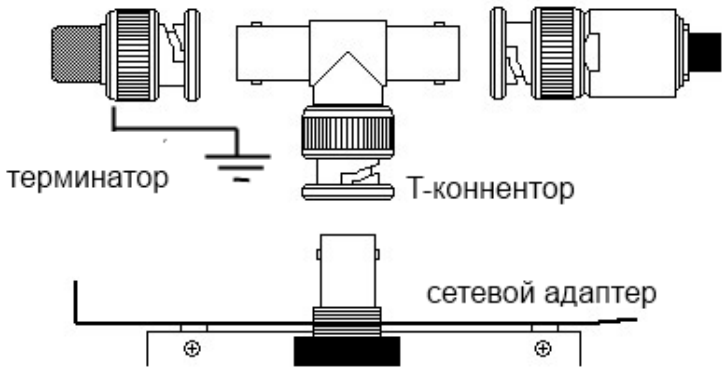


Рис. 2.18. Схема подключения рабочей станции на окончании сегмента

Физически терминатор представляет собой разъем с запаянным в нем, между центральным и внешним контактами, резистором. Сопротивление резистора должно равняться волновому сопротивлению кабеля. Для сетей типа 10Base-2 эта величина составляет 50 Ом. Только один терминатор в сегменте 10Base-2 может быть заземлен для уменьшения электромагнитных помех (может не заземляться при благоприятном электромагнитном окружении и небольшой, до 30 м, длине шины). Для заземления обычно используется терминатор с цепочкой и контактом на ее конце. Для 10Base-5 заземление одного и только одного из терминаторов (точнее, одной из точек сегмента) обязательно.

Сети на основе остальных стандартов имеют топологию, называемую *звезда*, хотя логически это шина (моноканал). Центром этой звезды является специальное устройство, называемое концентратор. Функционально это устройство аналогично повторителю в случае коаксиального кабеля. Преимущество топологии звезда по сравнению с общей шиной заключается в гораздо большей надежности. Нарушение целостности кабеля в первом случае приводит к изоляции от сети только одного компьютера, непосредственно подключенного к этому лучу, в то время как в случае общей шины изолируются все устройства на данном сегменте.

На рабочей станции сети Ethernet устанавливается специальная сетевая интерфейсная плата (**NIC — Network Inienace Card**). Эта плата предназначена для реализации функций приема и передачи данных. В варианте сети «тонкий Ethernet» устройство, которые осуществляет фактическую передачу данных в физическую среду (трансивер), выполнено на самой плате, а в сетях «толстый Ethernet» трансиверы располагаются непосредственно на кабеле и с сетевой платой соединены отдельным кабелем. Трансиверы генерируют электрические сигналы соответствующего уровня и передают их в коаксиальный кабель. Кроме того, трансиверы отвечают за прием сигналов из сети и обнаружение конфликтов. Трансиверы Ethernet обеспечивают также генерацию сигнала для тестирования качества передачи (SQE — Signal Quality Error), который часто называют «пульсом» (heartbeat). NIC считывает «пульс», чтобы проверить, нормально ли работает трансивер. «Пульсы» для трансиверов различных типов сетей Ethernet имеют разные временные параметры. Некоторые фирмы выпускают трансиверы, которые можно вручную настроить на тот или иной стандарт.

Для варианта сети 10Base-5 существует ограничение на допустимое число трансиверов - на одном сегменте кабеля можно размещать максимум 100 трансиверов с интервалом между ними минимум 2,5 м. Спецификация 10Base5 содержит также характеристики отводных кабелей, посредством которых NIC рабочей станции соединяется с трансиверами канала. Для классических сетей (где трансиверы не совмещены с NIC) разрыв отводного кабеля не вызывает отказа всей сети, поскольку приводит к отключению только соответствующей рабочей станции, однако зачастую трансиверы

были встроены в NIC, поэтому разрыв в кабельной системе приводит к отказу всей сети.

Стандарт 10Base-T определяет сеть Ethernet со скоростью 10 Мбит/с, строящуюся на базе двух неэкранированных витых пар (UTP) категории 5 с длиной сегмента не превышающей 100 метров. В стандарте 10BaseT предусмотрен контроль целостности канала и возможность отключения сегмента в случае отказа без отключения всей сети. Описание устройства доступа к среде передачи (MAU — Media Access Unit) в этом стандарте содержит несколько новшеств, отсутствующих в других спецификациях 802.3. Здесь предусмотрен контроль длительности передачи - если MAU продолжает передачу по истечении максимально допустимого промежутка времени, оно отключается. Выждав некоторое время, MAU включается вновь, и опять пытается осуществить передачу в сеть. Модуль проверки качества сигнала (SQE) рабочей станции контролирует работу MAU и обеспечивает его готовность к работе в сети. Повторители в сети типа 10BaseT могут отсоединять неправильно функционирующие MAU без отключения всех остальных рабочих станций. После устранения неисправности порт, который был отключен, вновь подключается к сети.

Важная особенность стандарта 10Base-T - интеллектуальная схема подавления, позволяющая сети l0Base-T функционировать в среде с широким диапазоном конфликтующих сигналов (речевых, сигналов цифровой сети с интеграцией обслуживания (ISDN), асинхронно передаваемых данных и т.д.). Система подавления, отфильтровывая «чужие» сигналы, позволяет обнаруживать полезные.

В стандарте 10Base-T решается еще одна проблема, связанная с искажением сигнала при прохождении по витой паре, что создавало существенные препятствия на пути создания высокоскоростной Ethernet. С целью ее решения был разработан специальный метод предварительной коррекции. Сигнал до начала передачи искусственно искажается таким образом, чтобы компенсировать изменения, возникающие в процессе передачи. В результате сигнал достигает пункта назначения в неискаженном виде.

В целом, преимущества l0Base-T заключаются в возможности использовать уже смонтированные (телефонные или другие) неэкранированные витые пары, в простоте монтажа и в более высокой надежности соединении по сравнению с вариантом Ethernet на коаксиальных кабелях.

Построение сети 10Base-T на концентраторах

Еще одно важное преимущество, появившееся в стандарте 10Base-T, которое и по сегодняшний день остается ключевым отличием новых локальных сетей – это принцип подключения каждого устройства к централизованной точке. В первых реализациях 10Base-T в качестве такой централизованной точки использовалось устройство, называемое **Ethernet-концентратором,** как показано на рис. 2.19.

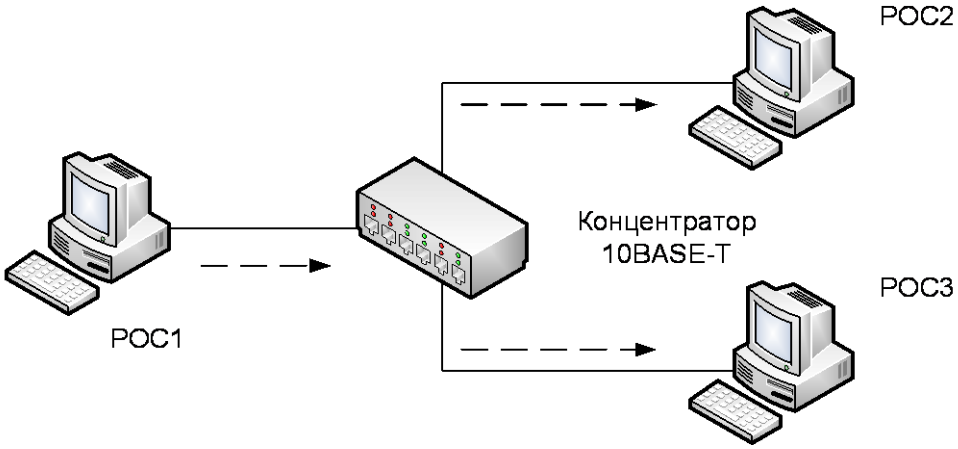


Рис. 2.19. Фрагмент сети Ethernet стандарта 10Base-T с использованием концентратора

Концентраторы – это, по сути, многопортовые повторители. Такое утверждение означает, что концентраторы просто регенерируют электрический сигнал, который приходит на один порт через все другие порты, т.е. концентратор повторяет полученную последовательность битов на всех портах кроме того, с которого был получен кадр.

Работая таким образом, концентраторы фактически создают электрическую шину, в точности как в 10Base-2 или 10Base-5. Следовательно, в таких сетях возможно возникновение коллизий и необходимо использовать алгоритм CSMA/CD. Этот алгоритм не предотвращает коллизии полностью, но позволяет продолжить работу даже в случае их возникновения. Когда происходит коллизия, алгоритм CSMA/CD обязывает устройства, вовлеченные в коллизию, отложить передачу данных на случайный интервал и затем повторить попытку. Такой подход позволяет локальной сети функционировать, но негативно сказывается на ее производительности. Стоит отметить два ключевых момента. Во-первых, алгоритм CSMA/CD обязывает устройства ожидать освобождения среды, прежде чем начать передачу. Такое требование помогает избежать коллизий, но также означает, что в каждый момент времени вести передачу информации может только одно устройство. В результате устройства, подключенные к одному концентратору, делят между собой общую полосу пропускания. Вторая основная особенность алгоритма – это метод обработки коллизий. Когда происходит коллизия, алгоритм обязывает устройства, вовлеченные в коллизию, отложить передачу на случайный период времени. Такое требование позволяет работать локальной сети, но в то же время понижает ее производительность.

Сети стандарта 10Base-T с использованием концентраторов решили несколько серьезных проблем, существовавших в сетях 10Base-2 и 10Base-5. Во-первых, существенно повысилась надежность работы сети. Повреждение одного кабеля или соединения могло привести и, как правило, при-

водило к неработоспособности всей сети на основе стандартов 10Base-2 и 10Base-5. В стандарте 10Base-T устройства подключаются отдельными кабелями к концентратору, следовательно, проблема одного кабеля затрагивает только одно устройство. Как уже отмечалось выше, использование кабеля витой пары в звездоподобной топологии (все кабели подключаются к центральному устройству) снижает стоимость самих кабелей и их прокладки.

Построение сети 10Base-T на коммутаторах

Все устройства в сетях 10Base-2 и 10Base-5 или любой сети с концентраторами могут испытывать коллизии, следовательно, все устройства в таких сетях находятся в одном домене коллизий.

Коммутаторы для локальных сетей значительно сокращают или даже полностью устраняют коллизии в сети. В отличие от концентраторов, коммутаторы не образуют общую электрическую шину и пересылают полученный сигнал на все свои порты. Они работают следующим образом:

- коммутаторы интерпретируют последовательность битов как кадр и в большинстве случаев пересылают такой кадр только в один порт, а не во все;
- если коммутатору необходимо переслать больше чем один кадр в один и тот же порт, коммутатор буферизует кадры в памяти и пересылает их последовательно один за другим, что позволяет избежать коллизий.

Избежать коллизии также помогает буферизация. Допустим, что компьютеры 1 и 2 одновременно посылают кадры компьютеру 3. Коммутатор знает, что одновременная передача кадров приведет к коллизии, поэтому один из кадров он буферизует (временно сохраняет его в памяти устройства) до тех пор, пока второй не будет целиком отправлен компьютеру 3.

Также следует отметить, что устройства, подключенные к одному порту коммутатора, не делят полосу пропускания с устройствами, подключенными к другим портам. Каждое устройство использует «выделенную» полосу пропускания. На практике коммутатор на 10 Мбит/с обеспечивает около 9,9 Мбит/с полосы пропускания на каждый порт. Это подчеркивает тот факт, что производительность сети значительно увеличивается. Например, концентратор, к которому подключено 24 устройства, на скорости 10 Мбит/с обеспечивает теоретически до 10 Мбит/с в общем. При использовании коммутатора вместо концентратора обеспечивается до 10 Мбит/с на каждый порт, что в сумме дает до 0,24 Гбит/с полосы пропускания. Таким образом, коммутаторы создают отдельный домен коллизий для каждого своего интерфейса и виртуальный маршрут для потока данных между двумя портами.

Рассмотренные выше ключевые концепции проиллюстрированы на рис. 2.20. На нем показаны те же самые рабочие станции, что и на рис. 2.19, но теперь они соединены посредством коммутатора, интерфейсы которого работают со скоростью 10 Мбит/с и создают 3 домена коллизий.

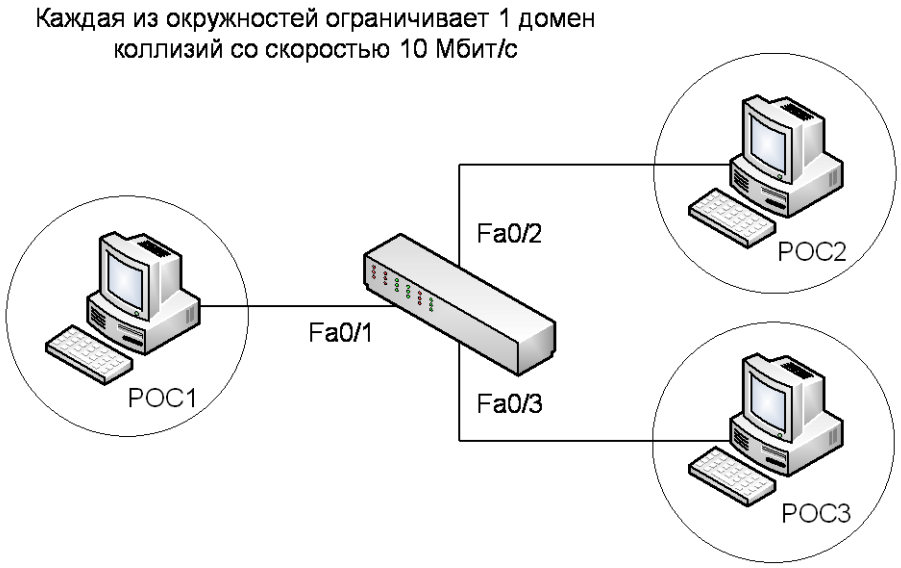


Рис. 2.20. Коммутатор разделяет три сегмента Ethernet и создает три домена коллизий

Поскольку коммутаторы буферизуют кадры в памяти, они могут полностью исключить коллизии в своих портах для одного устройства. В результате коммутаторы с единственным подключенным к порту устройством могут работать в дуплексном (full-duplex) режиме. Дуплексный режим означает, что сетевой адаптер может одновременно и принимать и передавать информацию. На рис. 2.21 показано, почему нет коллизии в дуплексном режиме, и как обеспечивается дуплексное подключение единственного компьютера к порту коммутатора.

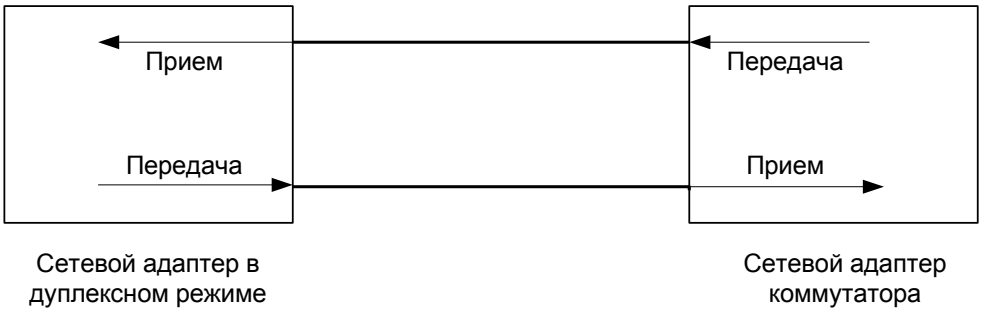


Рис. 2.21. Дуплексный режим работы коммутатора

Коллизия не может произойти между коммутатором и сетевым устройством в ситуации, показанной на рис. 2.19. Когда используется дуплексный режим работы, то в портах фактически отключается алгоритм CSMA/CD на обоих концах кабеля; ни одно устройство не ожидает отсут-

ствия сигнала в принимающей паре перед передачей данных. В результате такого подхода производительность Ethernet-сегмента удваивается за счет одновременного обмена информацией в обоих направлениях.

Рассмотрим подробнее принцип работы Ethernet-коммутатора.

Вполне очевидно, что основная задача коммутатора в локальной сети состоит в пересылке Ethernet-кадров. Для выполнения этой функции устройство использует определенные алгоритмы, основанные на анализе MAC-адресов отправителя и получателя в Ethernet-заголовках кадров. Следовательно, получив кадр из локальной сети, коммутатор должен принять решение: такой кадр следует переслать через какой-либо порт (порты) или проигнорировать (отбросить) его. Чтобы выполнить эту задачу, коммутаторы выполняют следующие действия:

1. Принимают решение о том, следует переслать кадр или отфильтровать (не пересылать) на основании MAC-адреса устройства-получателя.
2. Изучают MAC-адреса и строят таблицу коммутации на основании MAC-адресов устройств-отправителей кадров.
3. Поддерживают топологию второго уровня без петель с другими коммутаторами за счет использования протокола распределенного связующего дерева (Spanning Tree Protocol – STP).

Чтобы принять решение о том, следует ли пересылать кадр, коммутатор использует динамически создаваемую таблицу коммутации, в которой содержатся MAC-адреса и идентификаторы выходных интерфейсов. Коммутатор сравнивает MAC-адрес получателя кадров с записью в такой таблице, чтобы принять решение о том, следует ли передать кадр дальше или проигнорировать его.

Другой важной функцией коммутатора является механизм обнаружения MAC-адресов и построение таблицы коммутации для них. Если таблица коммутации устройства правильная и точная, коммутатор будет принимать правильные и точные решения об отправке и фильтрации кадров.

Коммутаторы строят таблицу адресов, просматривая входящие кадры и записывая из них MAC-адреса отправителей. Если на вход какого-либо порта устройства получен кадр и MAC-адрес в поле отправителя кадра отсутствует в таблице коммутации, коммутатор создает соответствующую ему запись в таблице. В таблицу помещается адрес и идентификатор интерфейса, через который был получен кадр. Когда коммутатор получает кадр с адресом получателя, отсутствующим в таблице, он пересылает такой кадр через все интерфейсы кроме того, откуда он пришел, в надежде, что искомое устройство окажется в каком-либо из подключенных к нему Ethernet-сегментов и ответит на такой кадр и, следовательно, можно будет внести правильную запись в таблицу MAC-адресов устройства. Процесс

пересылки кадров через все активные интерфейсы коммутатора, кроме того, откуда он пришел, называют **лавинной рассылкой** (flooding).

Третья главная функция коммутаторов локальных сетей заключается в предотвращении кольцевых маршрутов с помощью протокола распределенного связующего дерева (Spanning Tree Protocol – STP). Без протокола STP кадры могут бесконечно долго курсировать по кольцевому маршруту, если в Ethernet-сети есть резервные каналы. Чтобы избежать зацикливания кадров, протокол STP блокирует некоторые порты, и они не могут пересылать данные, при этом в сети между сегментами (доменами коллизий) существует только один активный маршрут для передачи данных. Результат работы протокола очевиден и прост: в сети остается один маршрут, зацикливания кадров не происходит, локальная сеть работает стабильно.

Выше было рассказано, как коммутатор принимает решение о том, переслать или отфильтровать кадр. Когда коммутатор принимает решение об отправке кадра, он может использовать один из механизмов пересылки, которые описаны ниже.

Большинство коммутаторов на сегодняшний день использует метод **коммутации с буферизацией кадров** (store-and-forward processing). При таком методе коммутатор получает кадр полностью, до последнего бита (сохраняет – store), а потом начинает его передачу (forward). Этот способ коммутации позволяет проверить целостность кадра посредством контрольной суммы (FCS) до его отправки.

Метод **сквозной коммутации** (cut-through). Коммутатор отправляет кадр, как только получена нужная информация – MAC-адрес получателя. Этот метод значительно уменьшает задержку, но кадры с неправильной контрольной суммой (FCS) не будут отброшены устройством.

Метод **бесфрагментной коммутации** (fragment-free processing). Коммутатор начинает передачу, как только получает первые 64 байта кадра. Этот метод позволяет исключить большинство ошибочных кадров при коммутации и в результате коллизий.

Основными характеристиками производительности коммутатора являются скорость фильтрации кадров, скорость продвижения кадров, общая пропускная способность по всем портам в мегабитах в секунду, задержка передачи кадра.

В заключение, приведем основные достоинства коммутаторов по сравнению с другими сетевыми устройствами (повторителями и концентраторами):

- Если к порту коммутатора подключено всего одно сетевое устройство, то он выполняет микросегментацию сети и предоставляет выделенную полосу пропускания для устройства.
- Коммутаторы позволяют осуществлять передачу множественных одновременных потоков данных между устройствами, подключенными к разным интерфейсам.

- Если к порту коммутатора подключено всего одно сетевое устройство, работающее в дуплексном режиме, то эффективная полоса пропускания удваивается.
- Коммутаторы выполняют согласование скорости, означающее, что устройства, подключенные посредством разных по скорости технологий Ethernet, могут взаимодействовать через коммутатор (через концентратор – не могут).
- Коммутаторы являются самообучающимися устройствами, так как строят таблицы продвижения автоматически на основе слежения за передаваемыми кадрами.

2.7.1. Технология Fast Ethernet

Fast Ethernet — спецификация IEEE 802.3, описывает стандарт протокола канального уровня для сетей, работающих при использовании медного или волоконно-оптического кабеля, со скоростью 100 Мбит/с. Спецификация является последователем стандарта Ethernet IEEE 802.3, используя тот же формат кадра, механизм доступа к среде CSMA/CD и звездную топологию. Изменения коснулись нескольких элементов конфигурации средств физического уровня, что дало возможность увеличить пропускную способность, включая типы используемого кабеля, длину сегментов и количество концентраторов.

Разница технологий FE и Ethernet находятся на физическом уровне (рис. 2.22). Уровни MAC и LLC в FE остались такими же и описываются также стандартами 802.3 и 802.2.

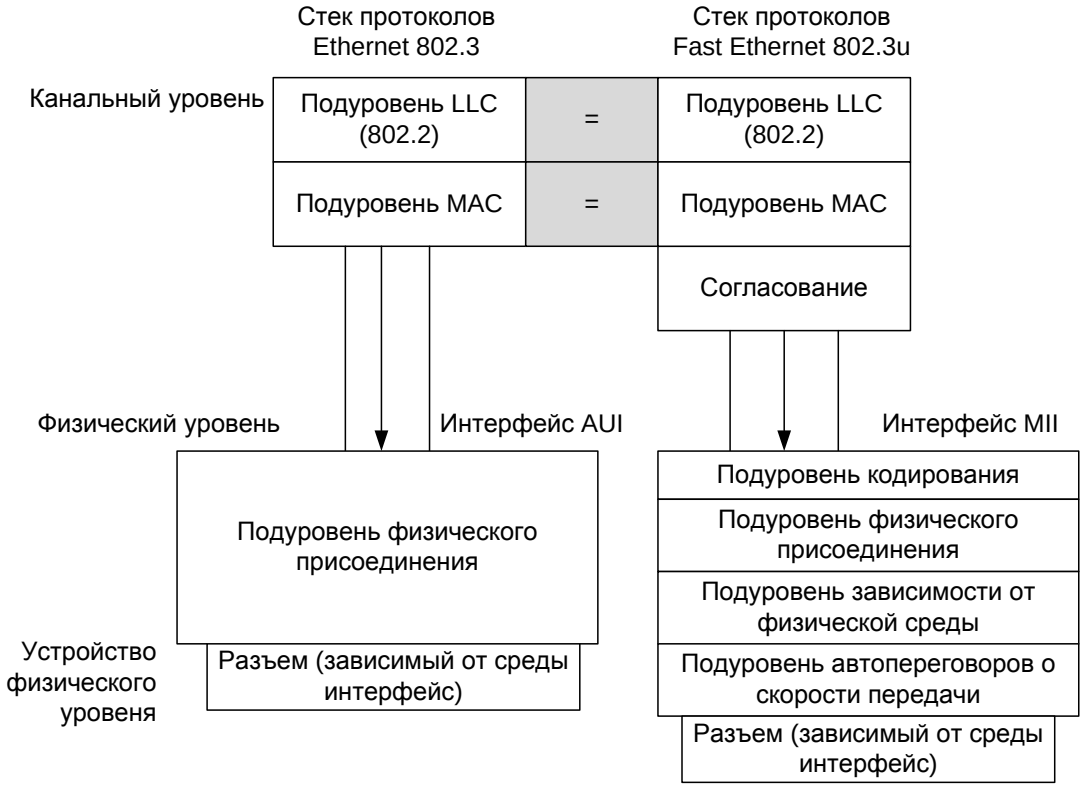


Рис. 2.22. Отличие технологии Fast Ethernet и Ethernet

Официально стандарт 802.3 установил три различных спецификации для физического уровня FE (рис. 2.23):

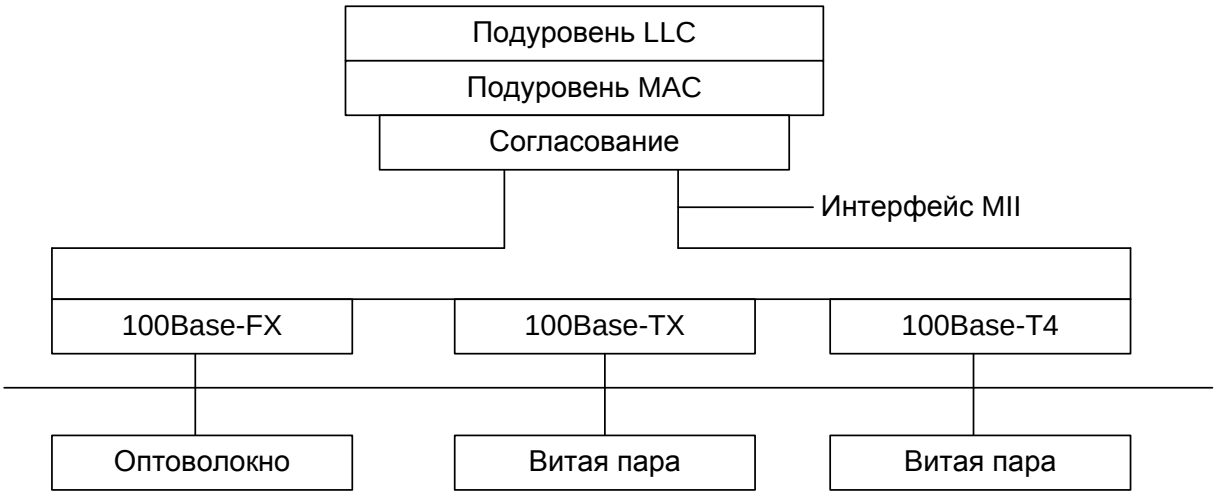


Рис. 2.23. Структура физического уровня Fast Ethernet

- **100Base-TX** — две витые пары проводов. Передача производиться в соответствии со стандартом передачи данных в физической среде, разработанным ANSI. Витой кабель для передачи данных может быть

экранированным или неэкранированным. Применяется алгоритм кодирования данных **4B/5B** и метод физического кодирования **MLT-3**.

- **100Base-FX** — две жилы ВОК. Передача тоже осуществляется в соответствии со стандартом передачи данных в волоконно-оптической среде, который разработан ANSI. Использует алгоритм кодирования данных **4B/5B** и метод физического кодирования **NRZI**.
- **100Base-T4** — особая спецификация, разработана комитетом IEEE 802.3u. Согласно этой спецификации передача данных осуществляется по четырем витым парам телефонного кабеля (UTP категории 3). Использует алгоритм кодирования данных **8B/6T** и метод физического кодирования **NRZI**.

Для всех стандартов справедливы перечисленные ниже утверждения и характеристики.

Форматы кадров технологии FE не отличаются от форматов кадров технологий 10-мегабитной сети Ethernet. Межкадровый интервал равен 0,96 мкс, а битовый интервал – 10 нс. Все временные параметры алгоритма доступа остались такими же.

Физический уровень Fast Ethernet включает в себя три элемента:

- MII – независимый от среды интерфейс (Media Independent Interface).
- Уровень согласования для того, чтобы уровень MAC, рассчитанный на интерфейс AUI, смог работать через MII с физическим уровнем.
- PHY – устройство физического уровня состоит из подуровней (подуровня логического кодирования, подуровней физического присоединения, подуровня автопереговоров).

2.7.2. Технология Gigabit Ethernet

Стандарт 802.3z принят 29.06.1998 г. на заседании комитета IEEE 802.3. Основная идея разработчиков стандарта Gigabit Ethernet заключается в максимальном сохранении идей классической технологии Ethernet при достижении битовой скорости в 1000 Мбит/с.

Стандарт GE на уровне протокола не поддерживает: качество обслуживания, избыточные связи, тестирование работоспособности оборудования и узлов.

В GE остаются все форматы кадров Ethernet и остается полудуплексная версия протокола, поддерживающая CSMA/CD. Можно использовать все основные виды кабелей: ВОК, витую пару 5 категории, экранированную витую пару.

Архитектура стандарта GE показана на рис. 2.24. В GE не существует универсальной схемы кодирования сигнала, которая была бы единой для всех физических интерфейсов. Для стандартов 1000Base-LX/SX/CX ис-

пользуется кодирование **8B/10B**, а для стандарта 1000Base-T используется код **PAM5**. Функцию кодирования выполняет PCS (подуровень кодирования), стоящий ниже интерфейса GMII (gigabit media independent interface). GMII обеспечивает взаимодействие между уровнем MAC и физическим уровнем.

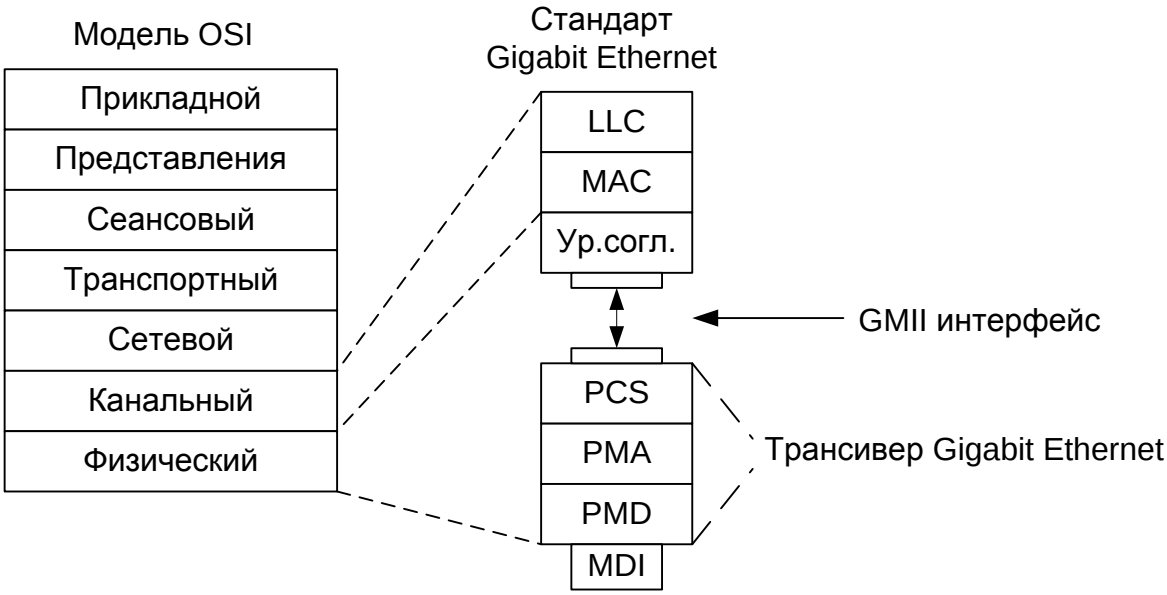


Рис. 2.24. Структура уровней стандарта Gigabit Ethernet, GMII интерфейс и трансивер Gigabit Ethernet

Окно коллизий (slot_time) зависит от размеров сегмента и должно быть больше, чем время двойного прохождения сигнала по среде передачи.

Для того, чтобы надежно обнаруживать коллизию при повышении скорости передачи есть два способа:

а) уменьшить длину сегмента коллизий, а, следовательно, и окно коллизий;

б) увеличить минимальную длину кадра.

При переходе от Ethernet к Fast Ethernet был уменьшен размер сегмента коллизий до 205 метров для UTP.

Для функционирования Gigabit Ethernet выбрали путь увеличения минимальной длины кадра до 416 байт (для 1000Base-X) или 520 байт (для 1000Base-T) путем добавления к нему расширения кадра (рис. 2.25). Различия в длине связаны с дополнительным логическим кодированием 8B/10B для 1000Base-X. Расширение кадра игнорируется (т.е. отбрасывается) на приемной стороне.

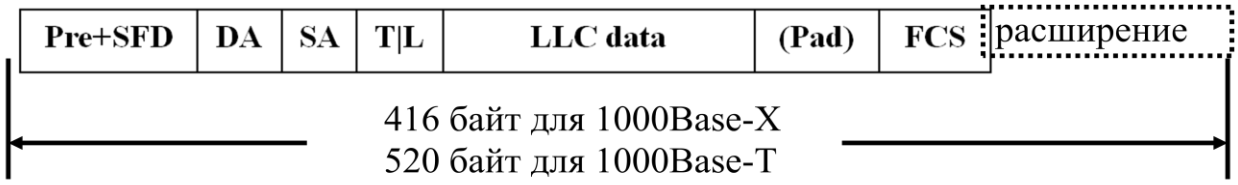


Рис. 2.25. Расширение кадра Gigabit Ethernet

Расширение кадра позволило избежать проблем с окном коллизий, но во многих случаях для маленьких пакетов приходится передавать слишком много ненужной информации (448 байт расширения из 520). Пропускная способность падает до скоростей Fast Ethernet.

Во избежание неполного использования канала передачи используется уплотнение кадров (рис. 2.26). Первый кадр передается, если нужно, с расширением, а вместо межкадровых промежутков (IFG), когда станция должна «молчать», она выдает в среду символы расширения (для того, чтобы другие станции не захватили среду), а затем после первого IFG следуют другие кадры, но уже без расширения. Промежутки между кадрами опять заполняются символами расширения. В этом случае полоса пропускания используется намного более практично. Fast Ethernet не поддерживают расширение и уплотнение передачи кадров.

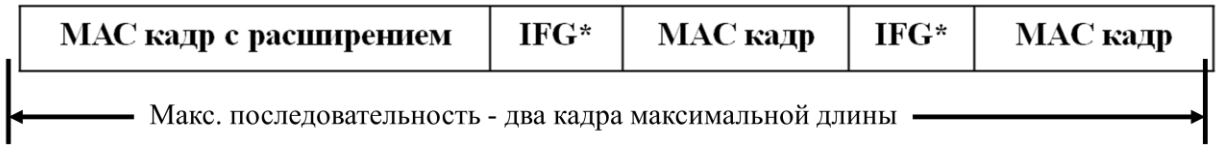


Рис. 2.26. Уплотнение передачи кадров Gigabit Ethernet

Стандарт Gigabit Ethernet определяет следующие среды передачи сигналов Ethernet со скоростью 1 Гбит/с:

- **1000Base-T** (IEEE 802.3ab) — стандарт, использующий UTP категорий 5e. В передаче данных участвуют 4 пары. Скорость передачи данных — 250 Мбит/с по одной паре. Используется метод кодирования **PAM5**, частота основной гармоники 62,5 МГц. Расстояние передачи до 100 метров.
- **1000Base-TX** разработан Ассоциацией Телекоммуникационной Промышленности и опубликован в 2001 году как «Спецификация физического уровня дуплексного Ethernet 1000 Мбит/с (1000Base-TX) симметричных кабельных систем категории 6 (ANSI/TIA/EIA-854-2001)». Стандарт, использует разделенную приемопередачу, что существенно упрощает конструкцию приемопередающих устройств. Еще одно существенное отличие 1000Base-TX является отсутствие схемы цифровой компенсации наводок и возвратных помех, вследствие этого сложность, уровень энергопотребления и цена процессоров становится ниже, чем у процессоров для построения сетевого оборудования стандарта 1000Base-T. Но для стабильной работы по этой технологии необходима кабельная система высокого качества, поэтому 1000Base-TX может использовать только кабель 6 категории, поэтому на основе этого стандарта практически не было создано промышленных разработок.

- **1000Base-X** — общий термин для обозначения стандартов со сменными приёмопередатчиками GBIC или SFP.
- **1000Base-SX** (IEEE 802.3z) — стандарт, использующий многомодовое волокно. Дальность прохождения сигнала без повторителя до 550 метров.
- **1000Base-LX** (IEEE 802.3z) — стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя зависит только от типа используемых приемопередатчиков и, как правило, составляет от 5 до 50 километров.
- **1000Base-CX** — стандарт для небольших расстояний (до 25 метров), использующий твинаксиальный кабель с волновым сопротивлением 75 Ом (каждый из двух волноводов). Заменен стандартом 1000Base-T и сейчас не используется.
- **1000Base-LH** — стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя до 100 километров.

2.7.3. Технология 10Gigabit Ethernet

Новый стандарт 10Gigabit Ethernet включает в себя 7 стандартов физической среды для LAN, MAN, WAN. Сейчас описывается стандарт поправкой IEEE 802.3ae и войдет в следующую ревизию стандарта IEEE 802.3, стандарт 10 Gigabit Ethernet определяет следующие среды передачи сигналов Ethernet со скоростью 10 Гбит/с:

- **10GBase-CX4** — технология 10-гигабитного Ethernet для небольших расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand.
- **10GBase-SR** — технология 10-гигабитного Ethernet для небольших расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое волокно. Он также поддерживает расстояния до 300 метров с использованием многомодового волокна.
- **10GBase-LX4** — использует уплотнение по длине волны для расстояний от 240 до 300 метров по многомодовому волокну. Также поддерживает расстояния до 10 километров при использовании одномодового волокна.
- **10GBase-LR** и **10GBase-ER** — стандарты поддерживают расстояния до 10 и 40 километров, при использовании многомодового и одномодового волокна соответственно.
- **10GBase-SW**, **10GBase-LW** и **10GBase-EW** — эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192 / STM-64 SONET/SDH. Они похожи со стандартами 10GBase-SR, 10GBase-LR и 10GBase-ER со-

ответственно, так как используют те же типы кабелей и расстояния передачи.

- **10GBase-T** (IEEE 802.3an-2006) — принят в июне 2006 года после 4 лет разработки. Использует экранированную витую пару. Расстояние передачи до 100 метров.

2.8. Виртуальные локальные сети

В современных сетях виртуальные логические сети - VLAN (Virtual Local Area Network) — главный механизм для создания логической топологии сети, не зависящей от её физической топологии.

С ростом и распространением локальных сетей Ethernet, на поверхность вышли ряд недостатков, которые ограничивают гибкость данной технологии и ее применимость для построения больших, разнесенных территориально локальных сетей. Необходимость построения таких сетей может возникать у средних и крупных предприятий и организаций для обеспечения взаимодействия между удаленными подразделениями. Итак, перечислим данные недостатки:

- невозможность ограничения передачи широковещательного трафика,
- невозможность группировки устройств на канальном уровне,
- привязка хостов локальной сети к физическому местоположению локальной сети,
- невозможность определение политик безопасности на уровне локальной сети.

Разберем каждый из них по отдельности:

Невозможность ограничения передачи широковещательного трафика

Действительно, локальная сеть, построенная на базе технологии Ethernet, образует широковещательный домен. Широковещательный трафик внутри такой сети будет передан всем узлам, что вытекает из самой архитектуры технологии и алгоритмов работы коммутаторов.

Невозможность группировки устройств на канальном уровне

В сети могут возникать ситуации, когда требуется ограничивать возможность доступа к определенным узлам. Для реализации таких ограничений используются списки доступа на коммутаторах, осуществляющих фильтрацию на основании MAC-адресов. Таким образом, для реализации списка доступа для группы устройств, необходимо прописывать правила отдельно для каждого из устройств, что усложняет конфигурирование сети и повышает нагрузку на коммутатор при большом количестве правил в таблице фильтров доступа.

Привязка хостов локальной сети к физическому местоположению локальной сети

На практике сети каких-либо крупных организаций представляют

собой совокупность сетей подразделений данных организаций. Если сотрудники подразделений находятся в одном помещении (например, на одном этаже) — проблемы доступа к ресурсам сети данного подразделения у них не возникает. Однако, часто встречается ситуация, когда некоторые сотрудники одного и того же подразделения располагаются в разных помещениях (например, на разных этажах здания). Для доступа таких сотрудником к ресурсам локальной сети необходимо тянуть кабель из основного помещения подразделения до рабочего места сотрудника. Такое решение представляется нерациональным как с точки зрения ограничения на длину сегмента Ethernet, так и с точки зрения расходов на прокладку кабеля.

Невозможность определение политик безопасности на уровне локальной сети

Данное ограничение естественным образом вытекает из первого и второго пунктов. Правила обработки пакетов на коммутаторах можно создавать только для отдельных устройств, передачу широковещательного трафика ограничить физически не возможно.

Для устранения вышеперечисленных, а также некоторых других недостатков современные локальные сети строятся на базе технологии VLAN.

VLAN — это группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. Устройства, находящиеся в разных VLAN, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору. Связь между этими устройствами возможна только на сетевом и более высоких уровнях. В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии.

VLAN — группа узлов сети, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам, и наоборот, устройства, находящиеся в разных VLAN, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях. За каждым портом коммутатора может быть закреплена конкретная VLAN, которая может быть логически сегментирована в соответствии с ее функциями и задачами. Порты одной VLAN имеют общий домен циркулярной рассылки. Порты, относящиеся к различным VLAN, не могут осуществлять циркулярную рассылку.

Цели разделения локальной сети на логические подсети:

- Разделение физической ЛВС на несколько логических подсетей
- Изолирование каждого порта для увеличения безопасности
- Изолирование широковещательного трафика

Можно повысить уровень безопасности путем сегментирования сети на отдельные домены циркулярной рассылки. Кроме того, можно регулировать размер и структуру домена путем регулирования размера и структуры VLAN.

VLAN позволяют группировать порты коммутатора таким образом, чтобы трафик ограничивался только членами той или иной группы. Данная функция ограничивает циркулярную, одноадресную и многоадресную рассылку (лавинная адресация) только портами, включенными в конкретную VLAN, что делает возможным эффективное разделение трафика, тем самым, обеспечивая более высокую пропускную способность.

История появления технологии

В 1984 году сотрудник одной из лабораторий компании Bellcore Дэвид Синкоски начал заниматься проблемой масштабируемости сетей, построенных на базе технологии Ethernet. Работавший в то время на скорости 10 Мб/с Ethernet был быстрее большинства аналогичных технологий того времени, однако из-за широковещательной архитектуры природы данной технологии не существовало хороших способов объединения множества таких сетей в единую сеть (построение «большой» сети Ethernet).

Как известно, сети Ethernet могут взаимодействовать друг с другом с помощью маршрутизатора IP. Однако в то время это не являлось решением проблемы, так как стоимость маршрутизаторов измерялась сотнями тысяч доллар, кроме того, их пропускная способность была значительно ниже пропускной способности коммутаторов сети Ethernet. Синкоски начал искать альтернативное решение, которое бы требовало меньше обработки в пересчете на пакет.

Проблема использования коммутаторов для отказоустойчивого соединения нескольких сетей Ethernet заключается в следующем: такая сеть требует избыточных соединения, что выливается в необходимость использования протокола на подобие STP (Spanning tree protocol, Протокол покрывающего дерева). Использование STP гарантирует, что в данный момент времени в сети существует только один активный путь от любого узла отправителя до любого узла получателя. Это выливается в возрастание нагрузки на коммутаторы, которые находятся в центре такой сети — получается, что пропускная способность составной сети ограничена пропускной способностью центральных коммутаторов, и ее никак не увеличить за счет организации дополнительных соединений между коммутаторами.

Чтобы обойти данную проблему Синкоски изобрел технологию VLAN: он добавил в кадр Ethernet новое поле - тег. На теги можно смотреть как на цвета, которыми окрашивают кадры: добавление тега окрашивает кадр. Далее, каждый коммутатор может быть настроен так, что будет обрабатывать кадры только определенного цвета и отбрасывать остальные. Таким образом, для каждой окрашенной сети может быть построено свое собственное покрывающее дерево. Из этого следует, что два коммутатора

могут быть соединены нескольким окрашенными сетями, и для каждой из сети будет существовать покрывающее дерево и активный путь, который не зависит от других окрашенных сетей. В итоге — мы увеличиваем пропускную способность участка сети между коммутаторами в число раз, равное числу окрашенных сетей, которые их соединяют.

Назначение VLAN

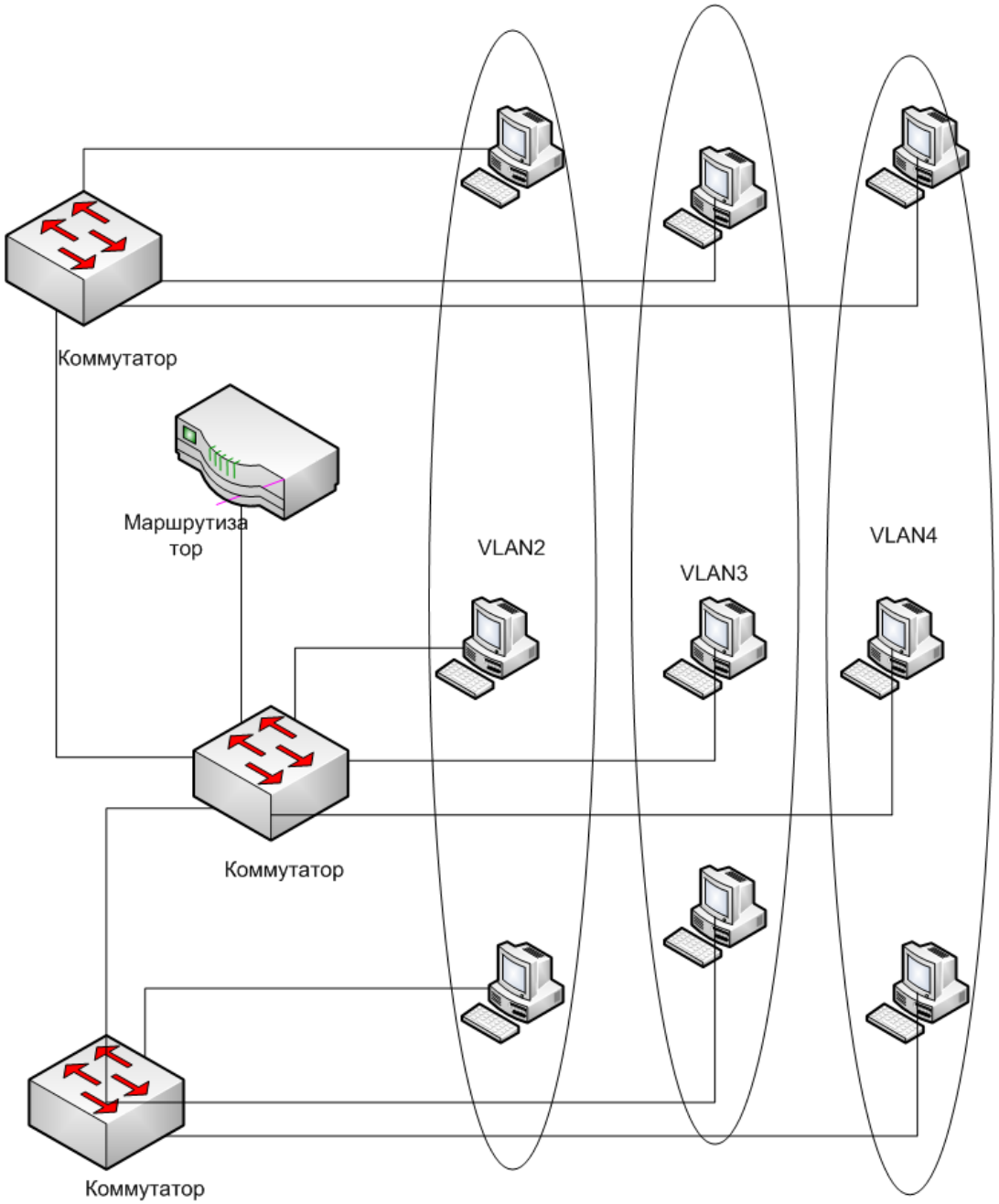


Рис. 2.27. Использование VLAN для создания изолированных сетей

В современных сетях технология VLAN уже не используется для достижения своей изначальной цели. В настоящее время основным назначением технологии VLAN является облегчение процесса создания изолиро-

ванных локальных сетей, которые затем обычно связываются между собой с помощью маршрутизаторов. Любая крупная современная сеть должна включать маршрутизаторы, иначе потоки ошибочных кадров (например, широковещательный трафик), будут затапливать всю сеть через прозрачные для них коммутаторы, приводя ее в неработоспособное состояние. Пример, построения такой сети можно увидеть на рис. 2.27.

До появления технологии VLAN для создания отдельной сети использовались либо физически изолированные сегменты коаксиального кабеля, либо не связанные между собой сегменты, построенные на повторителях и мостах. С помощью маршрутизаторов отдельные сегменты объединялись в составную сеть. Недостатки данного подхода уже были отмечены выше. Пример сети, построенной в соответствии с данным принципом, можно увидеть на рис. 2.28.

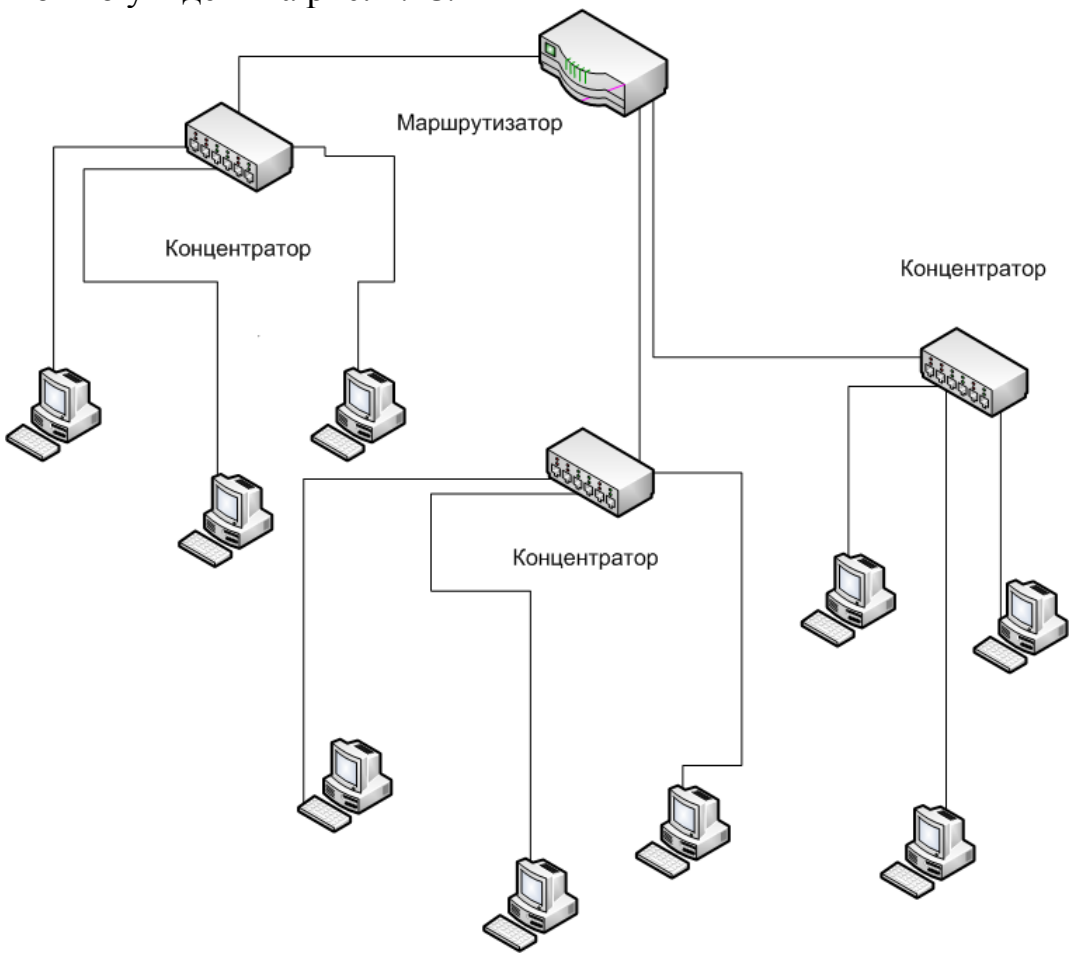


Рис. 2.28. Сеть на концентраторах

Долгое время технология VLAN не стандартизировалась, не смотря на то, что она уже была реализована в коммутаторах, выпускаемых разными производителями. Первый стандарт был принят организацией IEEE в 1998 году - IEEE 802.1Q. Текущая версия стандарта датируется 31 августа 2011 г.

В данном стандарте определяются базовые правила построения виртуальных локальных сетей, которые не зависят от протокола канального уровня, поддерживаемого коммутатором.

Способы организации VLAN

По способу организации виртуальные локальные сети делятся на две группы:

- статические VLAN,
- динамические VLAN.

В случае статической VLAN принадлежность хоста к той или иной виртуальной локальной сети определяется портом коммутатора, к которому подключен узел сети. В случае, если узел сети переключают на другой порт коммутатора, для сохранения доступа к виртуальной сети на коммутаторе необходимо внести порт в соответствующий VLAN, именно по этой причине данный способ получил название статический.

В случае динамических виртуальных локальных сетей принадлежность узла сети к VLAN определяется по специальному признаку - атрибуту. Таким признаком может выступать, например, MAC-адрес устройства, можно использовать и другие признаки для определения принадлежности устройства к VLAN (например, имя пользователя операционной системы и др.) При использовании динамического способа организации VLAN при переключении хоста на другой порт коммутатора никакой дополнительной конфигурации производить не требуется.

2.8.1. Виртуальные локальные сети на основе группировки портов

VLAN на основе группировки портов позволяет создавать VLAN из различных портов одного моста или коммутатора. Виртуальные локальные сети могут организовываться как на базе одного коммутатора, так и с использованием нескольких коммутаторов.

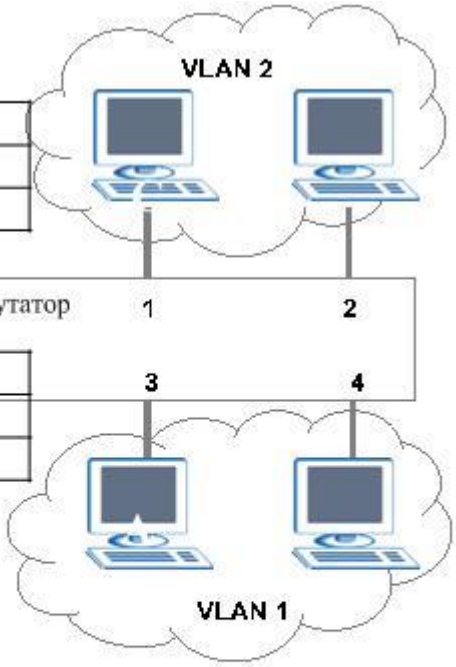
При создании VLAN на базе одного коммутатора обычно используется механизм группирования портов коммутатора. В этом случае каждый порт коммутатора приписывается к той или иной виртуальной сети, то есть порты группируются в виртуальные сети. Решение о продвижении сетевого пакета в этой сети основывается на MAC-адресе получателя и ассоциированного с ним порта. Если к порту, которому назначена принадлежность к определенной виртуальной сети, например к VLAN 1, подключить ПК пользователя, то этот ПК автоматически будет принадлежать сети VLAN 1. Если же к данному порту подключается коммутатор, то все порты этого коммутатора также будут принадлежать VLAN 1 (рис. 2.29). Технология VLAN на основе группировки портов в коммутаторах ZyXEL L2+ и L3+ позволяет управлять только исходящим трафиком. Таблицы коммутации при построении VLAN на основе группировки портов показаны на рис. 2.29.

Для VLAN 1:

Порт коммутатора	MAC-адрес хоста
1	A
2	B

Для VLAN 2:

Порт коммутатора	MAC-адрес хоста
3	C
4	D



Реальная таблица коммутации:

Порт коммутатора	VLAN	MAC-адрес хоста
1	1	A
2	1	B
3	2	C
4	2	D

Рис.2.29. Построение VLAN на основе группировки портов в коммутаторе

При использовании технологии группировки портов один и тот же порт может быть одновременно приписан к нескольким виртуальным сетям, что позволяет реализовывать разделяемые ресурсы между пользователями различных виртуальных сетей. Например, чтобы реализовать совместный доступ к сетевому принтеру или к файл-серверу пользователей виртуальных сетей VLAN 1 и VLAN 2, тот порт коммутатора, к которому подключается сетевой принтер или файл-сервер, нужно приписать одновременно к сетям VLAN 1 и VLAN 2.

Рассмотрим применимость данной технологии к построению виртуальной сети на базе нескольких коммутаторов (для упрощения ограничимся случаем двух коммутаторов): при передаче кадров между двумя коммутаторами информация о принадлежности к тому или иному VLAN теряется, т.к. в кадре Ethernet отсутствует поле, которое определяет принадлежность кадра к VLAN. Таким образом, на коммутаторах придется резервировать пару портов и привязывать ее к организуемой виртуальной сети, в случае организации *n* виртуальных сетей — резервировать придется *n* пар портов коммутаторов.

Таким образом, механизм группировки портов оказывается не эффективным при решении задачи создания виртуальных локальных сетей,

так как при построении виртуальной сети на базе нескольких коммутаторов необходимо только для организации VLAN задействовать столько портов коммутаторов и соединительных линий между ними, сколько организуется виртуальных сетей.

Настройка VLAN на основе группировки портов в коммутаторах ZyXEL представляет из себя матрицу, показанную на рис. 2.30, ячейки которой говорят о наличии связи между соответствующими портами.

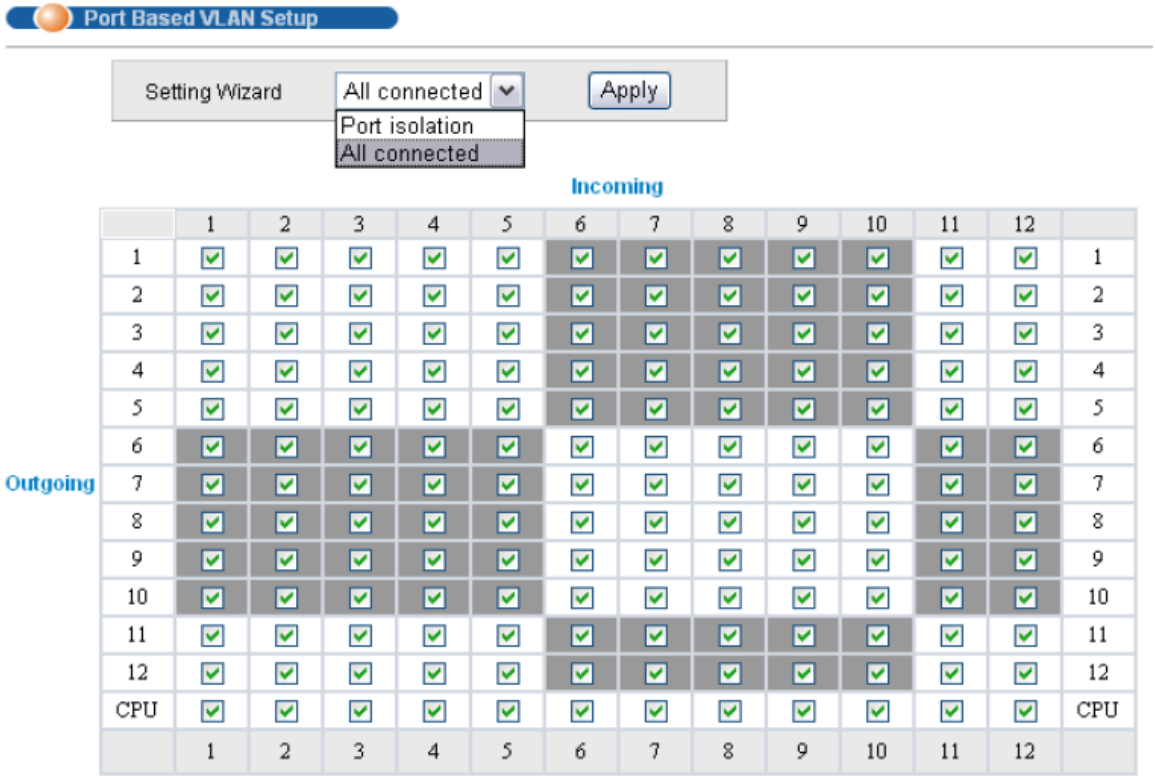


Рис. 2.30. Настройка VLAN на основе группировки портов

в коммутаторах ZyXEL

2.8.2. Виртуальные локальные сети на основе группировки MAC-адресов

При организации виртуальных сетей данным способом каждый известный коммутатору MAC-адрес приписывается той или иной виртуальной сети. При нахождении в сети множества узлов такой способ требует от администратора большого объема ручной работы: MAC-адреса должны быть промаркированы на каждом коммутаторе сети. В этом случае сам MAC-адрес становится меткой виртуальной сети.

2.8.3. Виртуальные локальные сети на основе стандарта IEEE 802.1Q

Вышеописанные подходы основаны только на добавлении дополни-

тельной информации к адресным таблицам коммутаторов, и в них отсутствует возможность встраивания в передаваемый кадр информации о принадлежности кадра к виртуальной сети. При добавлении этой информации в специальное поле кадра отпадет необходимость помнить на каждом коммутаторе о принадлежности всех MAC-адресов составной сети виртуальным сетям. Дополнительное поле с пометкой об идентификаторе виртуальной сети добавляется к кадру только при передаче между коммутаторами. При передаче кадра оконечному узлу данное поле удаляется. Это сделано для обеспечения совместимости нового стандарта со старым оборудованием, ведь изменяется только протокол взаимодействия между коммутаторами. Разные производители сетевого оборудования подходили к реализации данного решения по-разному. В итоге «мультивендорное» решение появилось после принятия IEEE стандарта 802.11Q.

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети, т.е. информация о принадлежности передаваемых Ethernet-кадров к той или иной виртуальной сети встраивается в сам передаваемый кадр (рис. 2.31).

До появления общепризнанного стандарта по организации виртуальных сетей IEEE 802.1Q каждый производитель сетевого оборудования использовал собственную технологию организации VLAN. Такой подход имел существенный недостаток — технологии одного производителя были несовместимы с технологиями других фирм. Поэтому при построении виртуальных сетей на базе нескольких коммутаторов необходимо было использовать только оборудование от одного производителя. Принятие стандарта виртуальных сетей IEEE 802.1Q позволило преодолеть проблему несовместимости, однако до сих пор существуют коммутаторы, которые либо не поддерживают стандарт IEEE 802.1Q, либо, кроме возможности организации виртуальных сетей по стандарту IEEE 802.1Q, предусматривают и иные технологии.

Рис. 2.31. Кадр Ethernet II и кадр 802.1Q содержащий принадлежность к VLAN

Стандартом IEEE 802.1Q в кадр вводится новый заголовок, к кадру

Ethernet добавляются 4 байта (рис. 2.32). TPID (Tag Protocol Identifier) – 2 байта, которые содержат информацию о принадлежности кадра Ethernet к протоколу 802.1Q и TCI (2 байта) - управляющая информация тега (Tag Control Information). Добавление четырех байтов к максимальному размеру кадра Ethernet ведет к возникновению проблем в работе многих коммутаторов, обрабатывающих кадры Ethernet аппаратно. Чтобы избежать их, группы по стандартизации предложили сократить на два байта максимальный размер полезной нагрузки в кадре. Спецификация IEEE 802.1p, создаваемая в рамках процесса стандартизации 802.1Q, определяет метод передачи информации о приоритете сетевого трафика. Стандарт 802.1p специфицирует алгоритм изменения порядка расположения пакетов в очередях, с помощью которого обеспечивается своевременная доставка чувствительного к временным задержкам трафика.

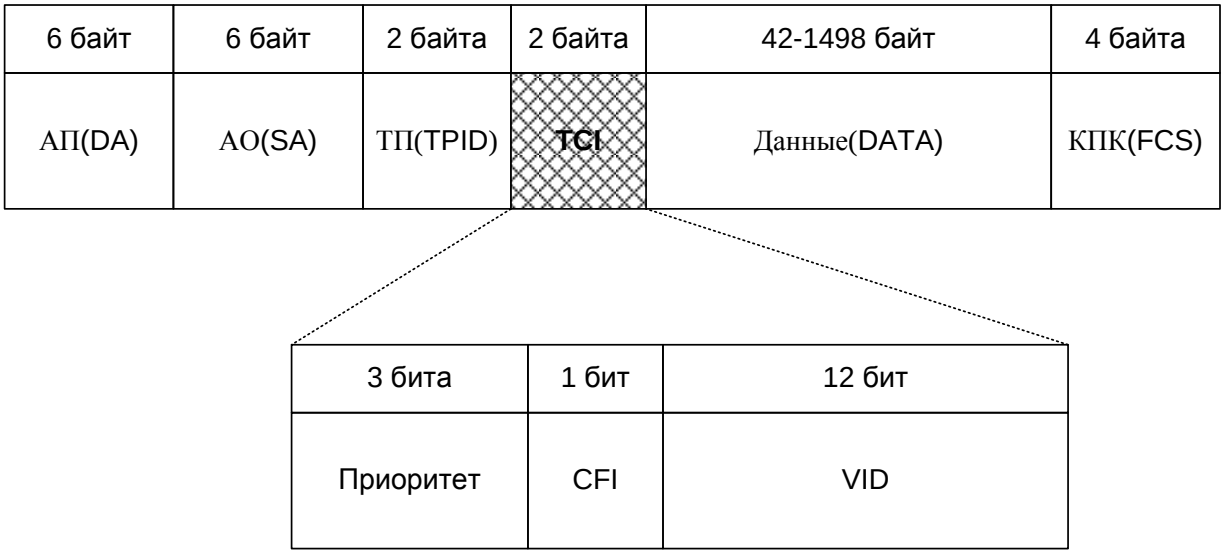


Рис. 2.32. Структура метки (Tag) в кадре Ethernet II

Метка IEEE 802.1Q (рис. 2.32) имеет следующие поля:

TPID: Признак идентификатора протокола, для 802.1Q TPID принимает значение 8100_{16} и полеTCI, которое содержит три поля:

- Поле Приоритет (User Priority). Возможно восемь значений (2^3) приоритета. Устройства, реализующие протокол IEEE 802.1P работает именно с этими 3 битами приоритета.
- Индикатор канонического формата, CFI (Canonical Format Indicator) - однобитовый флаг, который всегда равен 0 для кадров Ethernet. Если в поле Данные находятся данные других стандартов, не Ethernet, например Token Ring, то этот бит будет равен 1. Если кадр был получен с Ethernet порта и CFI равен 1, то этот кадр должен быть перенаправлен на untagged порт.
- VID – VLAN ID идентификатор VLAN, который и используется в стандарте 802.1Q. Это поле состоит из 12 бит и позволяет закодировать 4096

(2^{12}) значений VLAN. Из 4096 возможных значений, VID равные 0 и 4095 (FFF) зарезервированы, поэтому максимальное количество VLAN, которые работают в сети, равно 4094. VID = 0 определяет, что данный кадр не несет информации о VLAN, а несет только информацию о приоритете. VID = 4095 в оборудовании используется для внутренней коммутации.

Сетевые устройства, подключенные к портам с одинаковыми VID, могут взаимодействовать друг с другом и обмениваться кадрами.

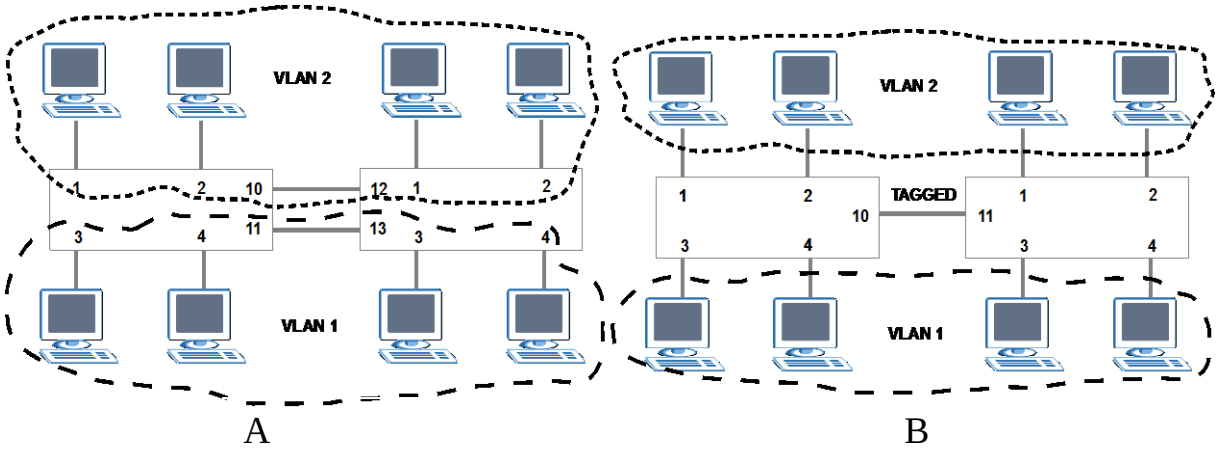


Рис. 2.33. Объединение узлов в разных VLAN на разных коммутаторах

Когда необходимо передать трафик одной-двух VLAN между коммутаторами, то схема, которая использовалась выше, выглядит нормально. Однако, когда количество VLAN возрастает, то схема явно становится очень неудобной, так как для каждой VLAN надо будет добавлять линк между коммутаторами для того, чтобы объединить хосты в один широковещательный сегмент (рис. 2.33 А), еще более усложняет схему организация VLAN в сети с несколькими коммутаторами.

Для решения этой проблемы используются тегированные порты, которые позволяют коммутатору передать трафик нескольких VLAN через один порт и сохранить при этом информацию о том, в пределах какой именно VLAN передается кадр (рис. 2.33 В).

Для упрощения конфигурации сети в стандарте 802.1Q вводятся два новых понятия.

Линия доступа – линия, которая связывает порт коммутатора (порт доступа) с хостом, принадлежащим к некоторой виртуальной локальной сети.

Транк – линия, соединяющая между собой порты двух коммутаторов. Через транк может передаваться трафик нескольких виртуальных сетей.

Коммутаторы, поддерживающие стандарт 802.1Q без специального конфигурирования, по умолчанию работают как стандартные коммутаторы, обеспечивая соединение всех со всеми. В сети, построенной на таких

коммутаторах, все конечные узлы относятся к сети VLAN с идентификатором vid=1. Все порты коммутаторов в сети по определению являются портами доступа. По VLAN 1 передаются непомеченные кадры.

Для выделения части узлов в отдельную виртуальную локальную сеть нужно выбрать для этой VLAN идентификатор, отличный от 1, далее настроить порты на коммутаторах, к которым подключены устройства, являющиеся оконечными узлами данной сети.

Порты доступа получают непомеченные кадры от оконечных узлов сети и окрашивают их, добавляя заголовок TCI. При передаче окрашенных кадров оконечному узлу (узлу назначения) заголовок TCI удаляется. Пример взаимодействия оконечных узлов такой сети можно увидеть на рис. 2.34.

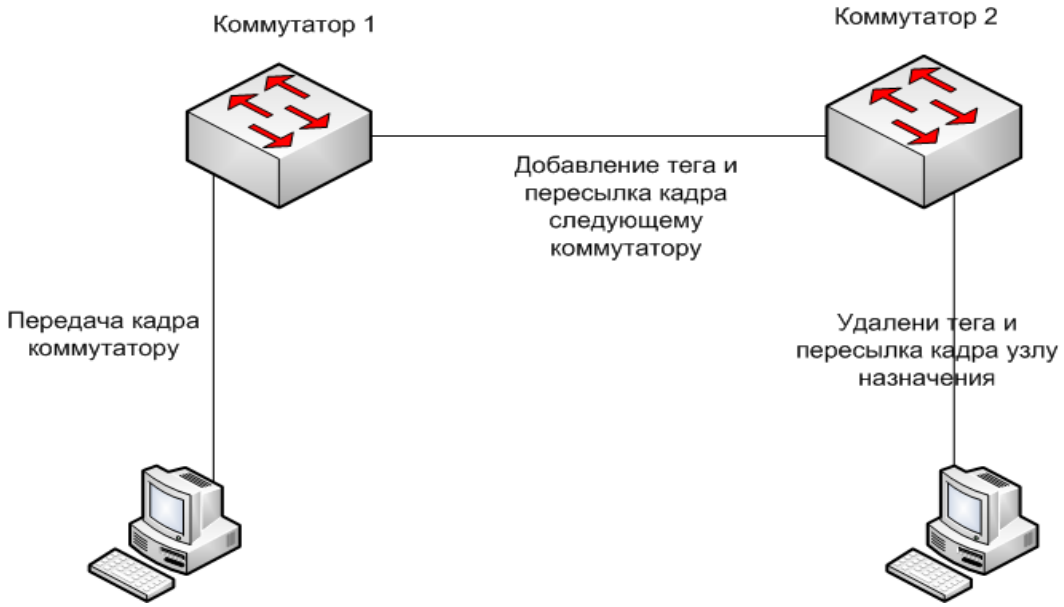


Рис. 2.34. Взаимодействие двух оконечных узлов виртуальной сети

Для присвоения портам идентификаторов VLAN согласно протоколу 802.1Q на Ethernet-коммутаторах производства фирмы ZyXel используется страница, показанная на рис. 2.35.

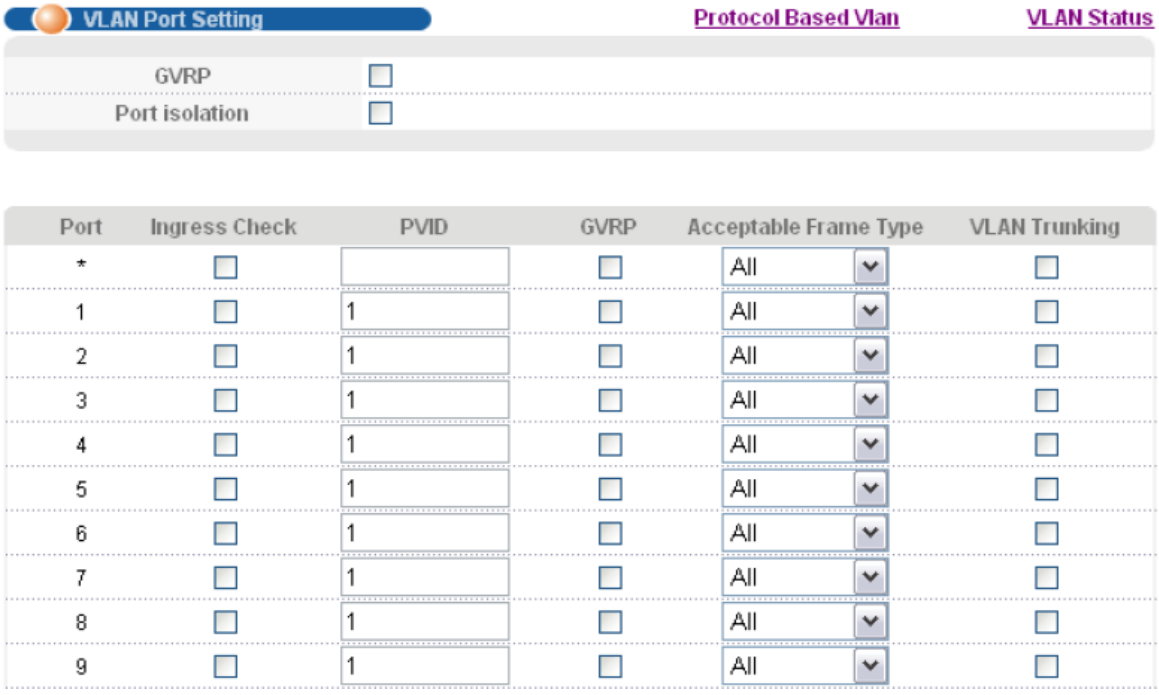


Рис. 2.35. Настройка портов для организации VLAN в коммутаторах ZyXEL

2.9. Локальные КСПД Token Ring

Локальная сеть **Token Ring** (маркерное кольцо) – это сеть без конкуренции между сетевыми устройствами, использующая метод доступа с передачей полномочий, логически представляющая собой кольцо, а физически - звезду. Реализуется она на базе стандартов ***IEEE 802.5, ISO 8802.5 и ECMA-89.*** Кабели к отдельным рабочим станциям образуют радиусы от концентратора (рис. 2.36). Исходная спецификация предусматривала скорость передачи 4 Мбит/с. В 90-х годах прошлого века практически все предлагаемые на рынке адаптеры были двухскоростными - на 4 и 16 Мбит/с.

Протокол подуровня MAC для сети позволяет использовать в качестве физической среды витую пару, коаксиальный или волоконно-оптический кабель. Однако в редакции ISO 8802.5 1987 г. рассмотрен лишь пример реализации физической среды на основе витой пары с обеспечением скоростей передачи 1...4 Мбит/с ± 0,01 %. Описываемые ниже параметры и характеристики ориентированы на этот тип физической среды.

Для предоставления сетевым станциям доступа к физической среде по кольцу циркулирует кадр маркера строго заданного формата. При получении кадра маркера станция анализирует его, модифицирует при необходимости и при отсутствии данных для передачи обеспечивает его дальнейшее продвижение к следующей станции. Станция, которая имеет дан-

ные для передачи, при обнаружении кадра маркера изымает его из кольца, что дает ей право на доступ к физической среде и передачу своих данных.

Станция, получившая право на передачу данных, выдает в кольцо кадр данных установленного формата последовательно по битам. При временной неготовности у такой станции данных для передачи она передает кадр-заполнитель (см. далее). Переданные данные проходят по кольцу всегда в одном направлении последовательно от одной станции к другой. Узел, выполняющий передачу, может захватить маркер на 10 мс, изъяв его из кольца, как показано на рис. 2.37. За это время узел может передать один или несколько кадров, причем максимальный размер кадра – 4 Кбайт для 4 Мбит/с, 16 Кбайт для 16 Мбит/с.

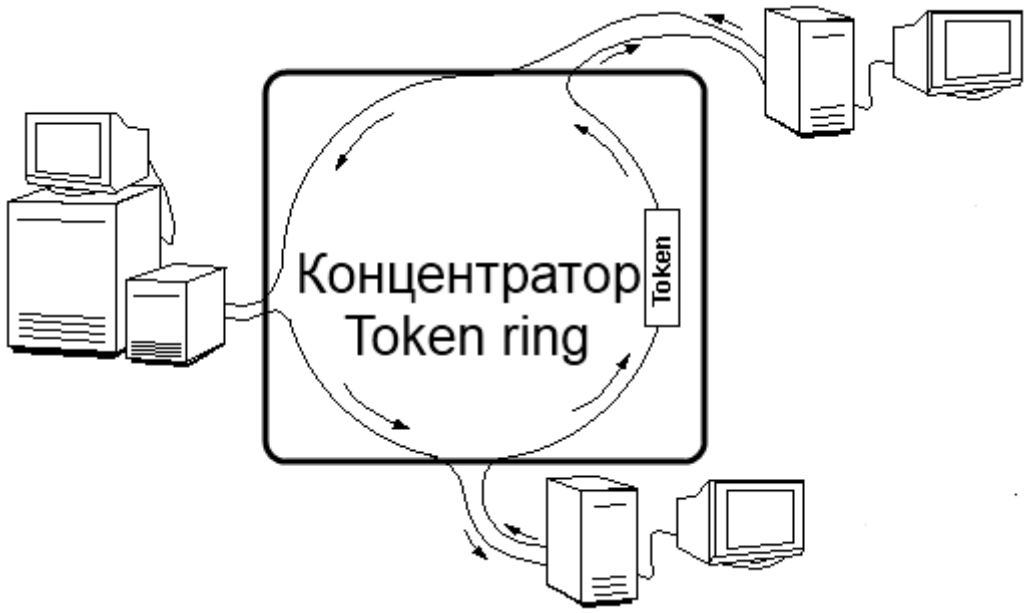


Рис. 2.36. Физическая конфигурация сети Token Ring

В версии 16 Мбит/с узел может освободить маркер сразу после завершения передачи кадра, такой алгоритм называется – алгоритм раннего освобождения маркера (Early Marker Release). В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно, так как по кольцу одновременно передаются кадры нескольких станций. Однако свои кадры в каждый момент времени может передавать только одна станция — та, которая владеет маркером доступа. Остальные станции в это время только повторяют чужие кадры, и принцип разделения кольца во времени сохраняется, ускоряется только процедура передачи маркера.

При поступлении кадра данных к адресуемой станции (станциям при широковещательной рассылке) эта станция «копирует» для себя этот кадр и выдает подтверждение приема. Станция, выдавшая кадр данных в коль-

цо, при обратном его получении с признаком подтверждения приема изымает этот кадр из кольца и выдает новый кадр маркера для обеспечения возможности другим станциям локальной сети передавать данные. Время удержания одной станцией маркера и занятости кольца ограничивается временем (тайм-аутом) удержания маркера.

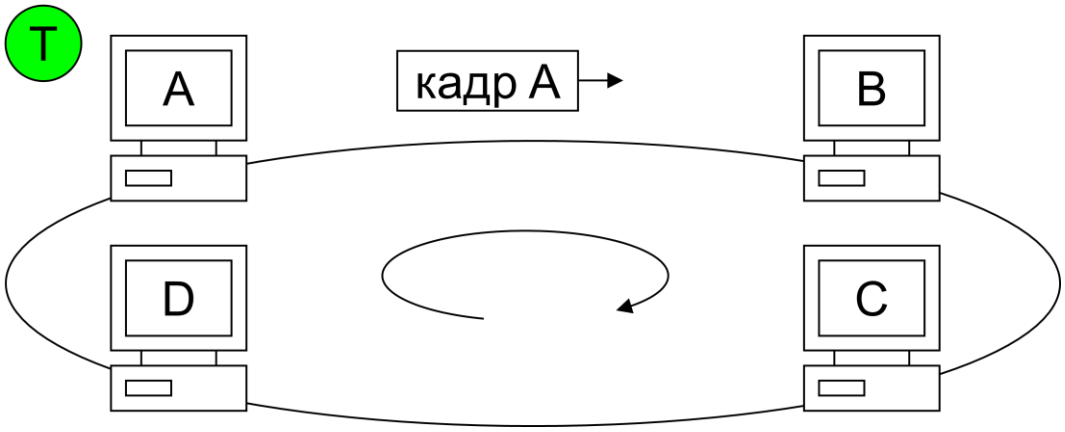


Рис. 2.37. Передача кадра в сети Token Ring

Каждая станция имеет также механизм обнаружения неисправностей сети, возникающих в результате ошибок передачи. Для реализации своего протокола подуровень MAC пользуется услугами физического уровня и диспетчера станции. В свою очередь, подуровень MAC обеспечивает услуги для подуровня LLC и диспетчера. Рабочие станции сети выполняют следующие функции:

- регенерацию сигнала (т.е. рабочая станция выполняет роль активного повторителя);
- преобразование маркера;
- прием кадра, формирование признаков распознаваемости адреса и факта копирования этого кадра;
- контроль ошибок функционирования сети и оповещение об этих ошибках остальных станций;
- выполнение одной станцией роли активного монитора (остальные станции в это время - неактивные мониторы, готовые при неисправности активного монитора выполнять его функции).

Для контроля сети один из узлов выполняет роль активного монитора, который выбирается при инициализации кольца, обычно это узел с максимальным MAC-адресом. Этот узел:

- создает маркер;
- удаляет дубли маркера и кадры, не удаленные источником;
- оповещает остальные узлы о своем присутствии, поскольку если в течение 7 секунд активный монитор не отправил специальный кадр, производятся его перевыборы.

Вся информация на уровне MAC передается в виде кадров или специального сообщения – заполнителя. Заполнитель должен передаваться до или после передачи кадров, маркеров и последовательностей прерывания, чтобы исключить неопределенность состояния передатчика. Заполнение может выполняться только нулями, только единицами или их комбинацией, с длительностью, определяемой таймером времени занятия среды.

В Token Ring существуют следующие форматы кадров:

- маркер,
- кадр данных,
- прерывающая последовательность.

Формат кадра стандарта IEEE 802.5 существенно отличается от формата кадра стандарта IEEE 802.3, поэтому невозможно просто соединять эти две сети между собой, даже если в обеих используется один и тот же способ передачи данных без модуляции несущей. В маркерном кольце применяются два основных формата: формат кадра маркера и формат кадра данных (рис. 2.38 и 2.39 соответственно).

Октеты	1	1	1
Поле кадра	НО	УД	КО

Рис. 2.38. Формат кадра маркера стандарта IEEE 802.5

	ПНК		Участвуют в формировании КПК					ПКК	
Октеты	1	1	1	6 (2)	6 (2)	MAC: 4..FFFF LLC: 0..133	4	1	1
Поле кадра	НО	УД	УК	АП	АО	Данные MAC или LLC	КПК	КО	СК

Рис. 2.39. Формат кадра данных стандарта IEEE 802.5

Назначения полей маркера и кадра данных следующие:

- **ПНК** - **последовательность начала кадра** (SFS - Start of Frame Sequence), включающая поля: начальный ограничитель и управление доступом.
- **НО** - **начальный ограничитель** (SD - Starting Delimiter), обозначает начало кадра и, представляя собой уникальную комбинацию бит (JK0JK000), не может быть распознан как данные. Физический уровень кодирует и передает четыре типа символов, представляемых ему подуровнем MAC: информационные (0 и 1); служебные (J и K). Эти символы передаются в среду в форме разностного манчестерского кода, который характе-

ризуется передачей двух элементов линейного сигнала на символ. При передаче бита «ноль» происходит изменение полярности сигнала в начале бита по отношению к полярности сигнала предыдущего бита, а при передаче бита «единица» не происходит изменения полярности. Передача служебных символов J и K отличается от описанного выше - оба сигнальных элемента символа имеют одну и ту же полярность. Поэтому здесь нет перехода в середине бита. Символ «J» имеет ту же полярность, что и последний сигнальный элемент предыдущего символа, а символ «К» имеет противоположную полярность. Чтобы избежать накопления постоянной составляющей, служебные символы обычно передаются в виде пар символов «J» и «К».

- **УД - управление доступом** (AC - Access Control), содержит биты «PPP» приоритета маркера ($\mathbf{P}_r$), бит «Т» маркера, бит «М» монитора и биты «RRR» приоритета резервирования ($\mathbf{R_r}$) (PPPTMRRR). Для того, чтобы показать, что рабочая станция хочет зарезервировать новый маркер, она может использовать один из восьми уровней приоритета (111 – высший, 000 – низший, причем приоритет 100 выше 001, то есть первый передаваемый бит является наиболее значащим). Бит Т=1 – для кадра, Т=0 – для маркера. Бит М=0 – для всех кадров и маркеров пассивного монитора, М=1 – для активного монитора.
- **УК - управление кадром** (FC - Frame Control), содержит информацию о типе «FF» данных кадра и биты управления «ZZZZZZ» (*FFZZZZZZ*). Биты FF=00 – определяют кадр MAC, FF=01 – определяют кадр LLC, FF=1x – резерв. Для кадра уровня LLC ZZZZZZ=rrrYYY, биты «rrr=000» – зарезервированы, биты «YYY» – приоритет протокольного блока данных LLC (Pm), принимают значения от 000 до 111. При приеме маркера или кадра станция сравнивают свой приоритет (Pm), с приоритетом (Pr) и (Rr), если Pm ≥ Pr станция захватывает маркер и начинает передачу, если Pm < Pr и Pm ≥ Rr, резервирует передачу. Для кадра уровня MAC значения битов ZZZZZZ определяют команды по управлению кольцом (табл. 2.10):
    - Команда **«Требования маркера»** служит для определения отсутствия активного монитора.
    - Команда **«Проверка дублированного адреса»** передается в процессе инициализации с адресом АП=АО. Если кадр возвращается с битом А=1 в байте СК, то в кольце есть еще одна станция с таким же адресом.
    - Команда **«Наличие активного монитора»** передается активным монитором после очистки кольца или по истечению таймера «активный монитор».
    - Команда **«Наличие пассивного монитора»** передается пассивным монитором после приема кадров «Наличие активного монитора» или «Наличие пассивного монитора» с битами А=0 и С=0 байта СК. Станция, которая копирует кадр с битами А=0 и С=0

байта СК, записывает адрес отправителя, как адрес вышестоящего соседа.

Таблица 2.10

Тип кадра	**Pm**	**УК (FC)**	**АП (DA)**	**VI**	**SVI-1**	**SVV-1**	**SVI-2**	**SVV-2**
Требование маркера	0	00 000011	Все станции	(0003)	(02) адрес вышестоящего соседа	адрес		
Проверка дублированного адреса	0	00 000000	Собственный адрес	(0007)				
Наличие активного монитора	Pr	00 000101	Все станции	(0005)	(02) адрес вышестоящего соседа	адрес		
Наличие пассивного монитора	0	00 000110	Все станции	(0006)	(02) адрес вышестоящего соседа	адрес		
Сигнальный кадр	0	00 000010	Все станции	(0002)	(02) адрес вышестоящего соседа	адрес	(01) тип сигн. кадра	(0001) (0002) (0003) (0004)
Очистка	0	00 000100	Все станции	(0004)	(02) адрес вышестоящего соседа	адрес		

- **«Сигнальный кадр»** передается при неисправности кольца. При получении этого кадра станция отключается от кольца и тестирует себя.
- Команда **«Очистка»** передается активным монитором вслед за кадром «Требование маркера» для повторной инициализации кольца при обнаружении бита М=1 байта УД или после истечения таймера «TVX - верная передача».

- **АП - адрес получателя** (DA - Destmation Address) и **АО - адрес отправителя** (SA - Source Address), содержат адрес получателя и адрес отправителя соответственно (рис. 2.40).

биты	1	1	46
поле	I/G	U/L	
адрес	**6-октетный**		

1	15
I/G	
2-октетный	

I/G=0 - индивидуальный адрес,

I/G=1 – адрес логической группы,

U/L=0 – глобально назначенный (индивидуальные адреса на множестве различных сетей различны и назначены глобально),

U/L=1 – локально назначенный (индивидуальные адреса назначаются каждой администрацией для своей локальной сети).

Рис. 2.40. Кодирование полей АП и АО

Каждая рабочая станция имеет уникальный 48-битный адрес, который записан в ПЗУ сетевой платы. Локальные адреса назначаются администратором локальной сети взамен глобального адреса, записанного в ПЗУ. Поля адресов рассчитаны на то, чтобы в них можно было записывать адреса рабочих станций из других кольцевых сетей или функциональную адресацию диспетчера. В частности, первые два (первый – для 16-битового адреса) байта 48-битового адреса каждого из упомянутых полей выделены под номер кольца станции, а первый бит третьего (второго) байта под признак функциональной (0) или групповой адресации (1). Комитет 802.5 предложил структуру адреса, в котором можно указывать множество колец, мостов и т.д., поэтому такая иерархическая адресация может быть очень сложной. Адрес кадра может содержать все нули («нулевой») – не предназначенный ни для одной станции или все единицы («широковещательный») – для всех станций сети.

- **Данные** – информация MAC, LLC или диспетчера. Формат поля «Данные» для кадра MAC представлен на рис. 2.41.

			Подвектор 1			…	Подвектор N		
октеты	2	2	1	1	m	…	1	1	m
поле	VL	VI	SVL	SVI	SVV	…	SVL	SVI	SVV

VL – длина вектора, **VI** – идентификатор вектора,

SVL – длина подвектора, **SVI** – идентификатор подвектора,

SVV – значение подвектора.

Рис. 2.41. Формат поля Данные для кадра MAC

- **КПК - контрольная последовательность кадра** (FCS - Frame Check Sequence), используется для обнаружения ошибок циклическим кодом с образующим полиномом 32 степени

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

- **ПКК - последовательность конца кадра** (EFS - End of Frame Sequence), включающая конечный ограничитель и состояние кадра.
- **КО - конечный ограничитель** (ED - Ending Delimiter), служит для определения станцией многокадровой передачи или ошибки (JK1JK1IE). Биты «J и K» – служебные, бит «I» – бит промежуточного кадра (I=1 – кадр промежуточный, I=0 –последний или единственный кадр), бит «E» – бит обнаружения ошибки (E=1 – ошибка, E=0 – нет ошибки).
- **СК - состояние кадра** (FS - Frame Status), указывает признак распознавания адреса «A» и копирования кадра «C» (ACrrACrr). Биты «r» – резерв. Кадры передаются со значением A=0 и C=0, если при приеме эти биты не изменились, то станция получателя отсутствует в кольце или кольцо неактивно. При приеме A=1 и C=0 – станция имеется, но кадр не скопирован; при A=1 и C=1 – кадр скопирован.

В маркерном кольце применяется также **Последовательность прерывания,** предназначенная для принудительного завершения передачи кадра и состоящая из двух байтов: начального и конечного ограничителей, причем биты E и I конечного ограничителя устанавливаются в 0.

2.10. Локальные КСПД FDDI (FDDI-II)

Технология **FDDI** (Fiber Distributed Data Interface) представляет собой оптоволоконный интерфейс распределенных данных. Является первой технологией локальных КСПД, в которой средой передачи данных является волоконно-оптический кабель. Работы по созданию технологий и устройств для использования волоконно-оптических каналов в локальных сетях начались в 80-е годы, вскоре после начала промышленной эксплуатации подобных каналов в территориальных сетях. Стандарт был разработан в середине 80-х годов Национальным Американским Институтом Стандартов и получил номер ANSI X3T9.5. Начальные версии стандарта FDDI обеспечивали передачу кадров со скоростью 100 Мбит/с по двойному волоконно-оптическому кольцу длиной до 100 км.

В 1979 году при Американском национальном институте стандартов (ANSI) была создана рабочая группа **X3T9.5** с целью разработки спецификаций высокопроизводительного канала ввода/вывода, названного локальным интерфейсом распределенных данных (LDDI - Local Distributed Data Interface). Однако после выдвинутой в октябре 1982 года на заседании группы идеи по использованию оптоволокна проект для LDDI был свернут, а рабочая группа была переориентирована на разработку стандартов для новой среды передачи сигналов. В это же время, на рубеже 80-х годов, некоторые компьютерные фирмы начали проводить эксперименты по построению высокоскоростных локальных сетей с использованием оптоволоконных линий. Так в 1982 году в фирме Burroughs разрабатывается специ-

альный протокол для сетей с кольцевой топологией: Timed Token Rotation Protocol (TTRP) — **протокол синхронизированного вращения маркера**. Одновременно корпорацией Sperry также были начаты работы по созданию 100 Мбит/с сети на базе оптоволоконных линий. Полученные Sperry результаты затем были переданы в ANSI, что в целом послужило началом официальной разработки стандарта FDDI.

Первый стандарт FDDI для протокола управления доступом к среде передачи сигнала (подуровень MAC) был опубликован в июле 1987 года (в стандарте ANSI X3.139-1987). В декабре 1988 года появился ANSI-стандарт для протокола физического уровня (PHY) — ХЗ.148-1988, а в июле 1990 года был опубликован стандарт для протокола физического уровня, зависящего от среды (PMD) — ХЗ.166-1990. В 1989-90-х годах данные стандарты FDDI для MAC, PHY и PMD становятся международными стандартами ISO (ISO 9314-2, ISO 9314-1, ISO 9314-3 соответственно). В 1992 году опубликована редакция 7.1 стандарта управления станцией (SMT – Station Management Standard), который определяет конфигурирование станции, конфигурирование кольца и средства управления, направленные на поддержку функционирования станций в кольце и, по сути, объединяет все ранее вышедшие стандарты в рамках единой архитектуры**.**

Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. Перечислим ее основные характеристики:

1) Используемая топология – кольцо, причем используется ее модификация – **двойное кольцо** – топология, построенная на двух кольцах. Первое кольцо (первичное) – основной путь для передачи данных. Второе (резервное) представляет собой резервный путь, дублирующий основной. При нормальном функционировании первого кольца, данные передаются только по нему. При его выходе из строя оно объединяется со вторым в одном из узлов, и сеть продолжает функционировать. Этот режим работы сети называется Wrap, то есть «свертывание». Данные при этом по первому кольцу передаются в одном направлении, а по второму в обратном, как показано на рис. 2.42.

2) Среда передачи – многомодовый оптоволоконный кабель (возможно применение медного кабеля – витой пары).

3) Максимальное количество узлов – 500.

4) Максимальная длина кольца – 100 км.

5) Максимальное расстояние между узлами – 2 км.

6) Скорость передачи – 100 Мбит/с (200 Мбит/с для полнодуплексного режима передачи).

7) Формат кадра данных – почти совпадает с форматом кадра Token Ring (отличается только формат кадра маркера).

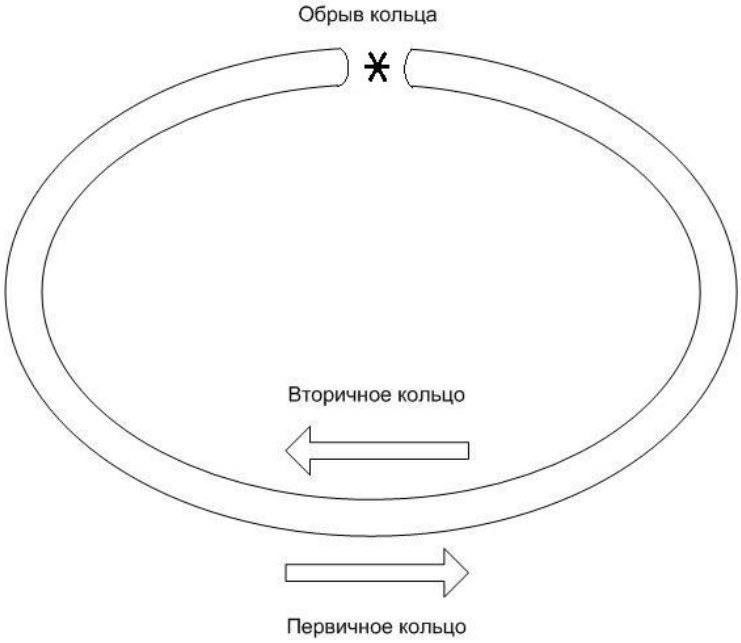


Рис. 2.42. Реконфигурация сети FDDI при отказе

Физический уровень разделен на два подуровня: независимый от среды подуровень PHY, и зависящий от среды подуровень PMD. Работу всех уровней контролирует протокол управления станцией (SMT – Station Management) (рис. 2.43).

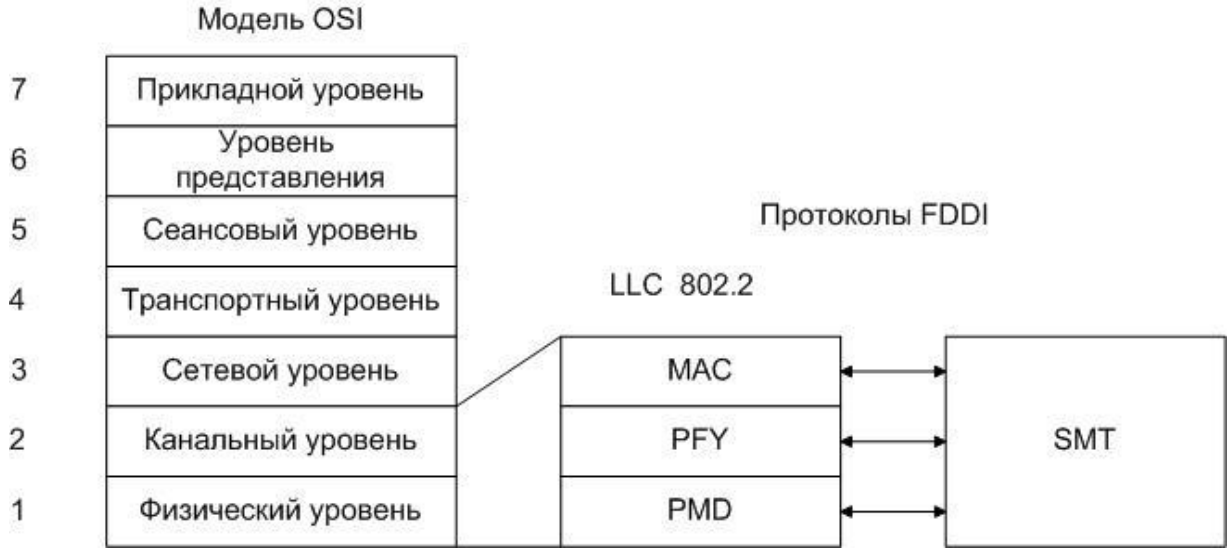


Рис. 2.43. Структура протоколов FDDI

Уровень PMD обеспечивает необходимые средства для передачи данных от одной станции к другой по оптоволокну. В его спецификации определяются:

- Требования к мощности оптических сигналов и к оптоволоконному кабелю.

- Параметры оптических разъемов MIC (Media Interface Connector), их маркировка.
- Длина волны в 1300 нанометров, на которой работают приемопередатчики.
- Представление двоичных сигналов в оптических волокнах в соответствии с методом кодирования NRZI.

Уровень PHY выполняет кодирование и декодирование данных, циркулирующих между MAC-уровнем и уровнем PMD, а также обеспечивает тактирование информационных сигналов. В его спецификации определяются:
- кодирование информации в соответствии методом кодирования 4B/5B;
- правила тактирования сигналов;
- требования к стабильности тактовой частоты 125 МГц.

Уровень MAC ответственен за управление доступом к сети, а также за прием и обработку кадров данных. В нем определены следующие параметры:
- Протокол передачи маркера.
- Правила захвата и ретрансляции маркера.
- Формирование кадра.
- Правила генерации и распознавания адресов.
- Правила вычисления и проверки 32-разрядной контрольной суммы.

Уровень SMT выполняет все функции по управлению и мониторингу всех остальных уровней стека протоколов FDDI. В управлении кольцом принимает участие каждый узел сети FDDI. Поэтому все узлы обмениваются специальными кадрами SMT для управления сетью. В спецификации SMT определено следующее:
- Алгоритмы обнаружения ошибок и восстановления после сбоев.
- Правила мониторинга работы кольца и станций.
- Управление кольцом, и переключение в аварийный режим работы Wrap, то есть «свертывание».

В табл. 2.11 представлены результаты сравнения технологии FDDI с технологиями Ethernet и Token Ring.

Для того, чтобы иметь возможность передавать собственные данные в кольцо (а не просто ретранслировать данные соседних станций), станция должна иметь в своем составе хотя бы один MAC-узел, который имеет свой уникальный MAC-адрес. Станции могут не иметь ни одного MAC-адреса, и, значит, участвовать только в ретрансляции чужих кадров. Но обычно все станции сети FDDI, даже концентраторы, имеют хотя бы один MAC. Концентраторы используют узел с MAC-адресом для захвата и генерации служебных кадров, например, кадров инициализации кольца, кадров поиска неисправности в кольце и т.п.

Таблица 2.11

Характеристика	FDDI	Ethernet	Token Ring
Битовая скорость	100 Мб/с	10 Мб/с	16 Мб/с
Топология	Двойное кольцо деревьев	Шина/звезда	Звезда/кольцо
Метод доступа	Доля от времени оборота токена	CSMA/CD	Приоритетная система резервирования
Среда передачи данных	Многомодовое оптоволокно, неэкранированная витая пара	Толстый коаксиал, тонкий коаксиал, витая пара, оптоволокно	Экранированная и неэкранированная витая пара, оптоволокно
Максимальная длина сети (без мостов)	200 км (100 км на кольцо)	2500 м	1000 м
Максимальное расстояние между узлами	2 км (-11 dB потерь между узлами)	2500 м	100 м
Максимальное количество узлов	500 (1000 соединений)	1024	260 для экранированной витой пары, 72 для неэкранированной витой пары
Тактирование и восстановление после отказов	Распределенная реализация тактирования и восстановления после отказов	Не определены	Активный монитор

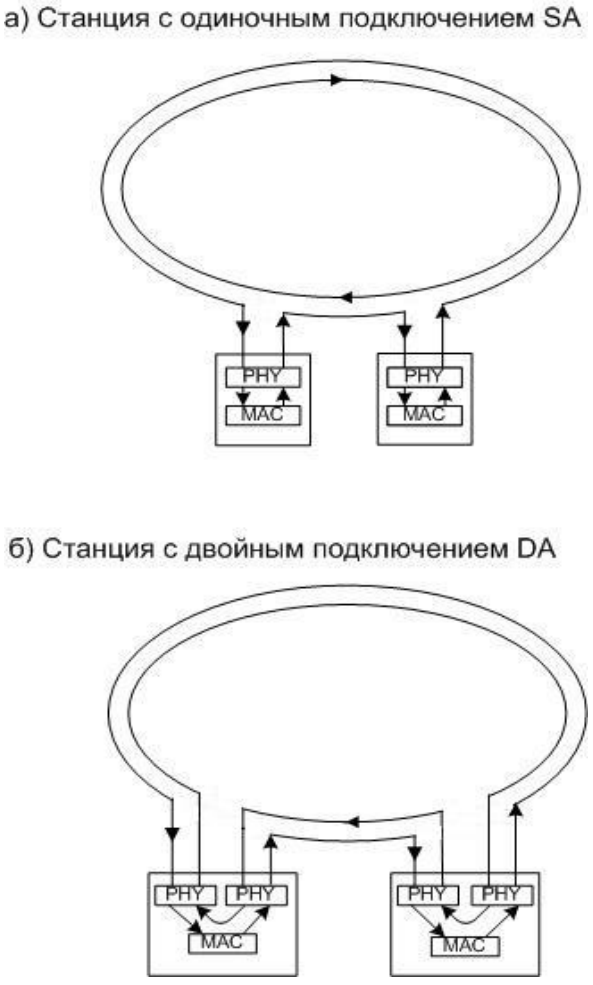


Рис. 2.43. Одиночное (SA) и двойное (DA) подключение станций

Станции, которые имеют один узел с MAC-адресом, называются **SM** (Single MAC) станциями (рис. 2.43, а), а станции, которые имеют два MAC, называются **DM** (Dual MAC) станциями (рис. 2.43, б), первый тип станций может быть подключен, как только к одному, так и к двум кольцам одновременно.

DM станции могут принимать данные одновременно по двум кольцам в полнодуплексном режиме, а при отказах участвовать в реконфигурации колец, как показано на рис. 2.44.

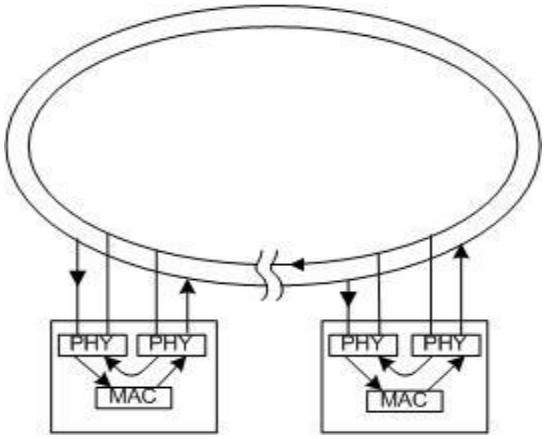


Рис. 2.44. Реконфигурация станций с двойным подключением при обрыве кабеля

Стремление обеспечить всестороннюю поддержку приложений реального времени стимулировало разработку стандарта **FDDI-II,** который реализует режимы, как пакетной коммутации, так и коммутации каналов. В соответствии с этим в стек протоколов был включен **протокол управления гибридным кольцом** (HRC - Hybrid Ring Control). Если для гибридного режима работы FDDI протокол физического уровня (PMD**)** остается без изменений, т.е. передатчики, кабель и системы соединений идентичны, то для протоколов MAC и PHY потребовалось внести некоторые изменения. С этой целью разработаны 4-я редакция стандарта ANSI для управления гибридным кольцом и редакция 4.1 протокола PHY-2, а также - редакция 4.1 протокола MAC-2.

Перечисленные стандарты были одобрены ISO и вышли в виде соответствующих международных стандартов ISO/IEC 9314-4 для SMF-PMD, ISO/IEC 9314-5 для HRC, ISO/IEC 9314-6 для SMT и ISO/IEC 9314-7 для PHY-2.

Кроме того, для сопряжения с оптоволоконными сетями стандарта синхронной оптической сети **SONET** (Synchronous Optical Network) ANSI был разработан стандарт **SPM** (SONET Physical layer Mapping), который задает отображение сигнала 125 Мбит/с физического уровня FDDI в син-

хронный транспортный сигнал уровня 3 (STS-3 Synchronous Transport Signal level 3) сети SONET.

На рис. 2.45 показана общая структура стандартов FDDI.

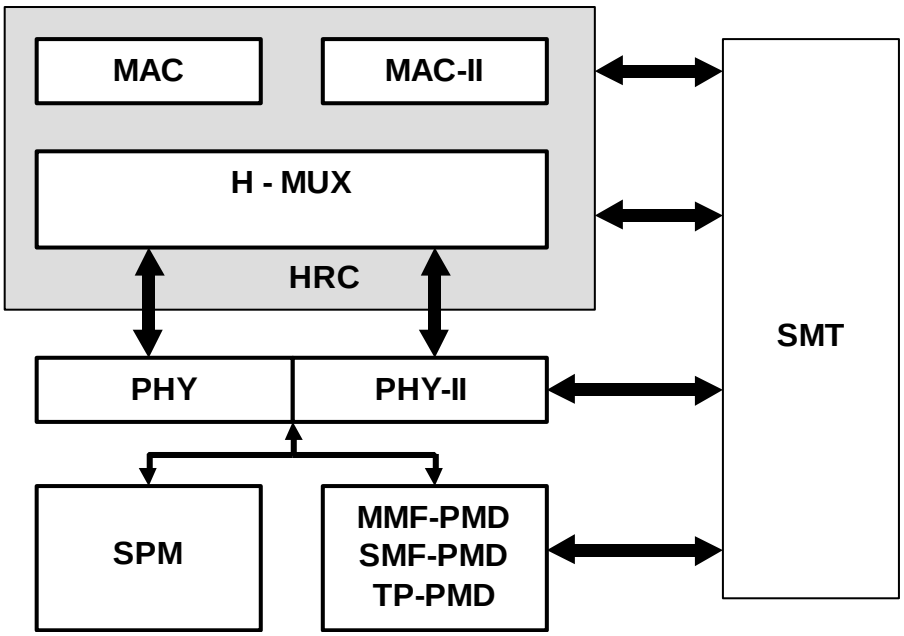


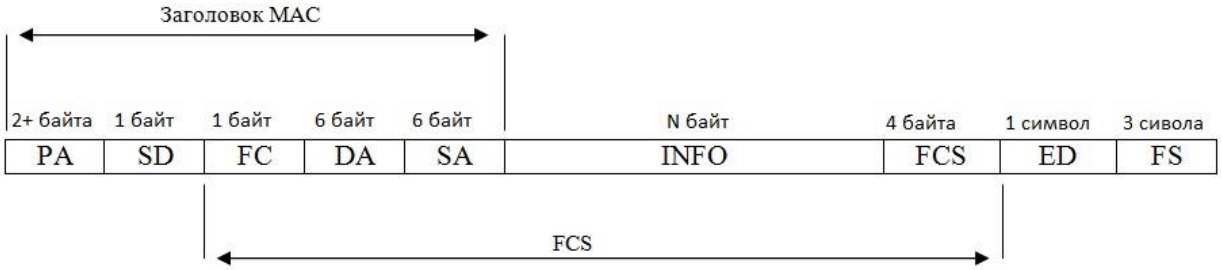
Рис. 2.45. Структура стандартов FDDI

Стандарт FDDI предусматривает максимум 1000 соединений (при расстоянии между станциями 2 км). Максимальная длина волоконно-оптического канала — 200 км. Для стандартного варианта FDDI используется многомодовый волоконно-оптический кабель диаметром 62,5 мкм с длинноволновыми (1300 нм) светодиодами в качестве источников. Каждая станция в сети FDDI функционирует как активный повторитель, поэтому сети FDDI могут достигать очень больших размеров без ухудшения характеристик сигнала.

Формат кадра FDDI аналогичен кадру стандарта IEEE 802.5 Token Ring и показан на рис. 2.46. Основное различие касается формата поля управления кадром. Старший разряд поля управления кадром (FC) определяет класс кадра: 0 — соответствует асинхронному, а 1 — синхронному кадру. Следующий по порядку разряд указывает на длину адреса, при этом 0 определяет 16-битный формат, а 1 — 48-битный формат. Следующий за этим два бита определяют формат кадра, а последние 4 бита являются битами управления.

В FDDI маркер представляет собой кадр данных очень малого размера. Он содержит поле класса кадра, которое идентифицирует данный кадр как маркер. Других полей, кроме начального и конечного ограничителей, в кадре маркера нет. Первый маркер обычно генерируется специально выбранной станцией. В FDDI для выбора такой станции используется схема конкурса заявок: каждая станция делает заявку на скорость вращения мар-

кера. Станция, имеющая заявку на более высокую скорость, становится победителем. Если две или более станций имеют одинаковые заявки, то победителем становится станция с наивысшим 48-битовым MAC-адресом.



где: PA - Преамбула: 16 или более пустых символов.

- SD - Стартовый разделитель: Символы 'J' и 'K'.
- FC - Frame Control: 2 символа, отвечающие за тип информации в поле INFO
- DA - Адрес назначения: 12 символов, показывающие кому адресован кадр.
- SA - Адрес источника: 12 символов, показывают адрес отправителя кадра.
- INFO - Поле данных: 0 до 4478 байтов информации.
- FCS - Контрольная сумма: 8 символов CRC.
- ED - Конечный разделитель: символ 'T'.
- FS - Конец кадра: 3 символа индикатор

Рис. 2.46. Формат кадра FDDI

2.11. Технология передачи 100VG-AnyLAN

Одновременно с разработкой технологии Fast Ethernet совместными усилиями компаний HP и AT&T была разработана технология передачи информации в стандартах Ethernet и Token Ring со скоростью 100 Мбит/с, получившая название **100-VG AnyLAN «**класс передачи речи» (VG - Voice Grade)**.** Данная технология, стандартизованная в дальнейшем IEEE (стандарт 802.12), сочетает в себе черты стандартов Ethernet и Token Ring, обеспечивает высокоскоростной обмен по неэкранированной (категория 3, 4 или 5), экранированной витой паре или оптическому волокну и не противоречит принципам построения и топологиям этих сетей. При этом расстояние между двумя узлами однообластной (содержащей единую область с пропускной способностью 100 Мбит/с) сети 100VG AnyLAN не должно превышать 2,5 км, что в целом достаточно для построения довольно крупных локальных сетей.

Основой принципиально новых широких возможностей 100VG-AnyLAN является использование звездообразной топологии, как на физическом, так и на уровне концепции построения сети. Центральным элементом сети, построенной по данной топологии, является интеллектуальный **DP-концентратор** (DP - Demand Priority), реализующий принцип коммутации кадров. Концентратор DP анализирует запросы на соединения,

поступающие от пользователей, и формирует на их основе управляющее воздействие для реализации процесса обслуживания заявок. Это позволяет оборудованию сети 100VG-AnyLAN минимизировать время ожидания обслуживания, максимизировать пропускную способность и обеспечить работу в сети приложений, критичных к временным задержкам (например, мультимедиа приложений). Отличительной особенностью сети, использующей режим DP, является обеспечиваемый высокий уровень безопасности передаваемой информации, который достигается самим принципом передачи, при котором пакет на входе концентратора поступает лишь на тот порт, к которому подключен абонент-получатель, что не реализуемо в существующих архитектурах сетей Ethernet, Token Ring и FDDI.

В технологии 100-VG AnyLAN используется не традиционный для Ethernet метод CSMA/CD, а другой метод доступа — метод обработки запросов по приоритету (demand priority). В этом случае всем узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, а затем разрешает этот запрос в соответствии с приоритетом (имеются два уровня приоритетов — высокий и низкий).

Для передачи данных по неэкранированным витым парам применяется технология квадратурного кодирования (quarief coding). Данные разбиваются на четыре параллельных потока, каждый из которых направляется по одной паре четырехпарного UTP-кабеля. В каждой паре проводов для передачи двух битов информации за один цикл применяется схема кодирования **5B6B** для скремблирования исходного потока данных и внешнего *NRZ*-кодирования данных при передаче в физической среде. Таким образом, квадратурное кодирование позволяет передавать по четырехпарному UTP-кабелю данные со скоростью 100 Мбит/с, при этом частоты сигналов в отдельных витых парах сохраняются на уровне не выше 25 МГц.

Для того, чтобы обеспечить передачу 100 Мбит/с по кабелю на экранированных витых парах, данные в сети 100-VG AnyLAN разбиваются на два параллельных потока. Этот метод позволяет воспользоваться преимуществом сравнительно высокого уровня защиты от помех (наводок от других кабелей), который обеспечивает экранированная витая пара, и передавать данные на более высоких частотах. В результате скорость передачи 100 Мбит/с достигается всего на двух парах проводов.

Недостатками технологии 100-VG AnyLAN являются: отход от традиционного метода CSMA/CD и несовместимость с существующими сетями Ethernet. Если технология 100-VG AnyLAN применяется для расширения работающей сети 10Base-T, то необходим мост для согласования скоростей передачи. Этот мост буферизует высокоскоростные пакеты, поступающие в менее скоростную сеть. Поскольку и в 10Base-T, и в 100BaseVG AnyLAN можно использовать один и тот же формат кадров, то не требует-

ся выполнение процедур преобразования пакетов и других операции по их обработке.

В табл. 2.12 приведены сравнительные характеристики технологии 100-VG AnyLAN с технологиями 10Base-T, и в 100Base-T.

Таблица 2.12

Технология		10BaseT	100BaseT	100-VG AnyLAN
Тополо-гия	Максимальный диаметр сети	2500 м.	8000 м.	412 м.
	Каскадирование концентраторов	3 уровня	5 уровней	2 концентратора (max)
Кабельная система	UTP Cat. 3, 4	100 м.	100 м.	100 м.
	UTP Cat. 3, 4	150 м.	200 м.	100 м.
	STP Type 1	100 м.	100 м.	100 м.
	Оптоволокно	2000 м.	2000 м.	412 м.
Технология	Кадры IEEE 802.3	+	+	+
	Кадры IEEE 802.5	-	+	-
	Метод доступа	CSMA/CD	DP	CSMA/CD+RSL (Reconciliation SubLevel)

Вопросы

1. Какой тип среды применяется в компьютерных сетях?
2. Приведите основные технологии локальных КСПД.
3. Дайте характеристику КСПД типа «тонкий» Ethernet.
4. Дайте характеристику КСПД типа «толстый» Ethernet.
5. Как называются заглушки, которые устанавливаются на концах шины из коаксиального кабеля?
6. С помощью чего ПК подключается к шине из коаксиального кабеля?
7. С помощью чего удлиняется кабельный сегмент шины из коаксиального кабеля?
8. Какую топологию имеет КСПД типа Ethernet на витой паре?
9. Какой кабель рационально использовать в новой кабельной системе для организации магистральной подсистемы?
10. Какой кабель рационально использовать в новой кабельной системе для организации вертикальной подсистемы?
11. Какие способы кодирования используется в сетях Ethernet и почему?
12. Объясните принцип работы метода доступа CSMA/CD.
13. Как сетевые платы могут обнаруживать коллизию?
14. Для чего служит и как формируется контрольная сумма пакета?
15. Вычислите пропускную способность внутренней шины коммутации, если коммутатор работает в неблокирующем режиме и имеет 8 FastEthernet-портов?
16. Укажите отличительные черты функционирования сетевых мостов и коммутаторов компьютерных сетей передачи данных?
17. Опишите основные отличия между способами доступа к разделяемой среде передачи данных по принципу CSMA/CD и CSMA/CA?
18. Изобразите кадр Ethernet-II 802.3 DIX, укажите длину и объясните назначение полей кадра?
19. Изобразите расширенный кадр Ethernet-II, содержащий тег VLAN ID принадлежности к определенной локальной виртуальной сети?
20. Укажите длину аппаратного адреса оборудования компьютерных сетей передачи данных? Объясните значение первых трех байт аппаратного адреса.
21. Объясните назначение следующих аппаратных адресов:
    00:00:00:00:00:00;
    FF:FF:FF:FF:FF:FF;
    01:00:00:00:00:00;
    01:00:0e:00:00:00;
    01:00:0e:00:00:00.
22. Что такое домен коллизий?
23. В чем состоят функции преамбулы и начального ограничителя кадра в стандарте Ethernet?

24. Чем объясняется, что минимальный размер кадра в стандарте 10Base-5 был выбран равным 64 байт?
25. Из каких соображений выбрана максимальная длина физического сегмента в стандартах Ethernet?
26. Опишите алгоритм доступа к среде технологии Token Ring.
27. Из каких соображений выбирается максимальное время оборота маркера по кольцу Token Ring?
28. В чем состоит сходство и различие технологий FDDI и Token Ring?
29. Какие элементы сети FDDI обеспечивают отказоустойчивость?
30. Технология FDDI является отказоустойчивой. Означает ли это, что при любом однократном обрыве кабеля сеть FDDI будет продолжать нормально работать?
31. К каким последствиям может привести двукратный обрыв кабеля в кольце FDDI?
32. Что общего в работе концентратора l00VG-AnyLAN и обычного моста?
33. Из-за увеличения пропускной способности минимальный размер кадра в Gigabit Ethernet пришлось увеличить до 512 байт. В тех случаях, когда передаваемые данные не могут полностью заполнить поле данных кадра, оно дополняется до необходимой длины неким «заполнителем», который не несет полезной информации. Что предпринято в Gigabit Ethernet для сокращения накладных расходов, возникающих при передаче коротких данных?
34. С чем связано ограничение, известное как «правило 4-х хабов»?

РАЗДЕЛ 3. ПРОТОКОЛЫ СЕТЕВОГО УРОВНЯ В ЛОКАЛЬНЫХ КСПД

При описании сетевого уровня затрагиваются такие понятия, как логическая адресация, фрагментация, маршрутизация и другие. Если на втором уровне ЭМВОС решаются задачи внутри отдельно взятой сети, то протоколы третьего уровня в системе передачи данных должны определять универсальные форматы пакетов информации в сети и обеспечивать правила их маршрутизации при передаче из одной сети в другую. Таким образом, сетевой уровень обеспечивает как внутрисетевое, так и межсетевое взаимодействие хостов на основе логической адресации, предоставляя канальному уровню информацию для работы с их физическими адресами. С этой целью был разработан протокол IP, на основе которого строится адресация в современных локальных и глобальных сетях. Рассмотрим данный протокол подробнее.

3.1. Протокол IP

Подробное описание протокола IP, относящегося к третьему уровню ЭМВОС, приведено в документе RFC 791.

Протокол IP (Internet Protocol – межсетевой протокол) предназначен для использования в соединенных между собой компьютерных сетях обмена данными на основе коммутации пакетов. Он обеспечивает передачу блоков данных, называемых дейтаграммами, между отправителем и получателем, хосты которых идентифицируются адресами фиксированной длины.

Необходимо отметить, что данный протокол ограничивается доставкой дейтаграмм через систему соединенных между собой сетей. При этом он не поддерживает механизмов повышения надежности сквозной доставки, управления потоком данных, сохранения порядка и других функций, общепринятых для протоколов прямого взаимодействия между хостами.

Задачей протокола IP является перемещение дейтаграмм через множество сетей. Эта задача решается путем передачи дейтаграмм от одного модуля IP к другому, пока дейтаграмма не будет доставлена адресату. Модули IP размещаются на хостах и маршрутизаторах (шлюзах). Процесс выбора пути к адресату принято называть маршрутизацией.

Дейтаграммы маршрутизируются от одного модуля IP к другому через промежуточные сети на основе интерпретации адресов IP. Поэтому, одним из важнейших механизмов IP является адресация.

При маршрутизации сообщений от одного модуля IP к другому может потребоваться передача дейтаграмм через сети, для которых максимальный размер пакета меньше размера дейтаграммы. Для решения этой

проблемы протокол IP обеспечивает механизмы фрагментации и сборки дейтаграмм.

Таким образом, основные функции протокола IP – адресация, фрагментация и сборка дейтаграмм (в том случае, если они имеют большой размер и сеть не позволяет передать их целиком).

3.2. Модули IP

Как было сказано выше, модули IP используются всеми хостами и маршрутизаторами, участвующими в сетевом обмене данными. Для данных модулей характерны общие правила интерпретации полей адреса, фрагментации и сборки дейтаграмм. Также необходимо отметить их роль в маршрутизаторах, где они выполняют процедуры принятия решения о пересылке дейтаграмм. Физически модуль IP представляет собой программу, которая обеспечивает выполнение задач, присущих протоколу IP. Для примера рассмотрим простейший сценарий передачи дейтаграммы от одного хоста к другому через один промежуточный маршрутизатор.

На передающем хосте запущена программа, которая является источником данных. Она подготавливает эти данные и вызывает локальный модуль IP для передачи их в виде дейтаграммы, указывая адрес получателя и другие параметры. Модуль IP, в свою очередь, готовит заголовок дейтаграммы и присоединяет к нему данные. После этого модуль IP определяет локальный сетевой адрес для указанного получателя. На этой стадии таким адресом является адрес маршрутизатора. Модуль передает дейтаграмму и адрес маршрутизатора локальному сетевому интерфейсу канального уровня. Интерфейс канального уровня создает заголовок и присоединяет к нему дейтаграмму IP, формируя кадр, который передается в локальную сеть.

Дейтаграмма приходит на маршрутизатор в кадре канального уровня. Интерфейс канального уровня удаляет заголовок канального уровня и передает дейтаграмму модулю IP. Модуль IP определяет на основе IP-адреса, что дейтаграмму следует переслать хосту другой сети. Тогда модуль IP определяет адрес канального уровня для пересылки дейтаграммы хосту-адресату и вызывает интерфейс канального уровня той сети, куда будет передаваться дейтаграмма. Интерфейс канального уровня создает заголовок и, присоединив к нему дейтаграмму, передает сформированный кадр хосту-адресату.

На хосте получателя дейтаграмма выделяется из кадра интерфейсом канального уровня и передается модулю IP. Модуль IP определяет по заголовку, что дейтаграмма адресована программе на данном хосте и передает ей данные из дейтаграммы вместе с адресом отправителя и другими параметрами.

Фрагментация дейтаграмм требуется в тех случаях, когда дейтаграмма приходит из сети, которая поддерживает больший размер пакетов, чем промежуточные сети на пути следования дейтаграммы к получателю.

Процесс фрагментации длинной дейтаграммы выполняется модулем IP (например, на маршрутизаторе). При этом из одной дейтаграммы создается две новых дейтаграммы. Содержимое полей заголовка исходной дейтаграммы копируется в заголовки новых дейтаграмм. Данные исходной дейтаграммы делятся на две части по 64 битовой границе. Вторая часть дейтаграммы может иметь размер, не кратный 64 битам, но первая часть должна содержать целое число 64 битных блоков (NFB – Number of Fragment Blocks – число блоков фрагментации).

Первая часть дейтаграммы помещается в первую из созданных дейтаграмм, ее поле длины в заголовке устанавливается в соответствии с длиной первой дейтаграммы. Также в заголовке первой дейтаграммы устанавливается флаг наличия дополнительных фрагментов.

Вторая часть данных помещается во вторую из созданных дейтаграмм, ее поле длины в заголовке устанавливается в соответствии с длиной новой дейтаграммы. В ее заголовке указывается значение поля смещения, увеличенное на величину NFB. Значение флага наличия дополнительных фрагментов сохраняется в соответствии с флагом исходной нефрагментированной дейтаграммы.

Описанную процедуру фрагментации можно с легкостью применить для разбиения дейтаграммы на n фрагментов, если $n > 2$.

Сборка фрагментов дейтаграммы осуществляется модулем IP (например, на хосте-получателе) и предполагает объединение дейтаграмм, имеющих в заголовках одинаковые значения полей идентификации, адреса отправителя и получателя, а также протокола транспортного уровня. Объединение осуществляется путем размещения данных из каждой дейтаграммы в позицию буфера, указанную полем смещения фрагмента в заголовке дейтаграмм. Первый фрагмент будет иметь нулевое смещение, а для последнего фрагмента нулевое значение будет иметь флаг more-fragments.

3.3. Структура IP пакета IPv4

В дальнейшем дейтаграмму, сформированную на основе протокола IP, будем называть IP-пакетом. Информация, содержащаяся в начале IP-пакета, помимо данных, составляет заголовок IP-пакета. Общепринятая структура заголовка IP пакета версии IPv4 подробно описана в документе RFC 791 (рис. 3.1).

Рис. 3.1. Структура заголовка IPv4

- **Версия** – для IPv4 значение поля равно 4.
- **IHL** (Internet Header Length) – длина заголовка IP-пакета в 32-битных словах. Это поле указывает на начало блока данных в пакете. Минимальное корректное значение для этого поля равно 5.
- **ToS** (Type of Service) – тип обслуживания. Используется для индикации желаемого качества сервиса и представляет собой набор параметров. Как правило, индикация ToS используется маршрутизаторами для выбора реальных параметров передачи применительно к данной сети, следующего интервала сети или следующего маршрутизатора при доставке IP-пакета.
  - **0, 1, 2 биты** – приоритет (precedence) данного IP-пакета;
  - **3 бит** – требование ко времени задержки (delay) передачи IP-пакета (0 – нормальная, 1 – низкая задержка);
  - **4 бит** – требование к пропускной способности (throughput) маршрута, по которому должен отправляться IP-пакет (0 – низкая, 1 – высокая пропускная способность);
  - **5 бит** – требование к надежности (reliability) передачи IP-пакета (0 – нормальная, 1 – высокая надежность);
  - **6, 7 биты** – ECN – явное сообщение о задержке (управление IP-потоком). На практике в большинстве случаев это поле равно 0.
- **Длина пакета** – длина пакета в октетах, включая заголовок и данные. Минимальное корректное значение для этого поля равно 20, максимальное 65535.
- **Идентификатор** – значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета. Для фрагментированного пакета все фрагменты имеют одинаковый идентификатор.

- **Флаги**
  - **1 бит** – всегда равен 0;
  - **2 бит** – DF (don't fragment) определяет возможность фрагментации пакета;
  - **3 бит** – MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов.
- **Смещение фрагмента** – значение, определяющее позицию фрагмента в потоке данных. Смещение задается количеством блоков размером 8 байт.
- **TTL** (Time to live) – определяет максимальный срок существования IP-пакета. Это значение устанавливается отправителем и уменьшается в каждой точке на пути доставки, где IP-пакет подвергается обработке. Так при прохождении маршрутизатора TTL уменьшатся на единицу. Если значение TTL становится нулевым до того, как IP-пакет будет доставлен адресату, то такой пакет будет уничтожен.
- **Протокол транспортного уровня** – идентификатор протокола более высокого уровня указывает, данные какого протокола содержит пакет, например, TCP, UDP или ICMP.
- **Header Checksum** – контрольная сумма заголовка. Обеспечивает возможность проверки корректности переданного пакета, вычисляется в соответствии с документом RFC 1071. Если при передаче IP-пакет был поврежден, то вычисленная контрольная сумма заголовка принятого пакета не совпадет с содержащимся в его поле значением контрольной суммы, и пакет будет отброшен как ошибочный. Таким образом, протокол IP не обеспечивает механизма гарантированной доставки. В нем не предусмотрены механизмы подтверждения доставки или средства контроля ошибок (за исключением контрольной суммы заголовка), а также средства повтора передачи и управления потоком данных.
- **IP-адрес отправителя** – IP-адрес сетевого интерфейса хоста-отправителя IP-пакета. Имеет длину 32 бита.
- **IP-адрес получателя** – IP-адрес сетевого интерфейса хоста-получателя IP-пакета. Имеет длину 32 бита.
- **Options** – опции. Обеспечивают дополнительные функции (временные метки, параметры безопасности и специальные средства маршрутизации).

Отметим, что каждый IP-пакет является независимым элементом и не связан с другими IP-пакетами.

3.4. Адресация IPv4

Схема адресации протокола IPv4 подробно описана в документах RFC 990 и RFC 997. Физически IP-адрес – это уникальная 32-разрядная последовательность. Для удобства работы принято разделять его на 4 байта, каждый из которых представляют в десятичном виде. Полученные числа разделяют точками.

Приведем для примера настройку параметров сетевого интерфейса в операционной системе Windows NT. Настройка производится в свойствах сетевого подключения (рис. 3.2).

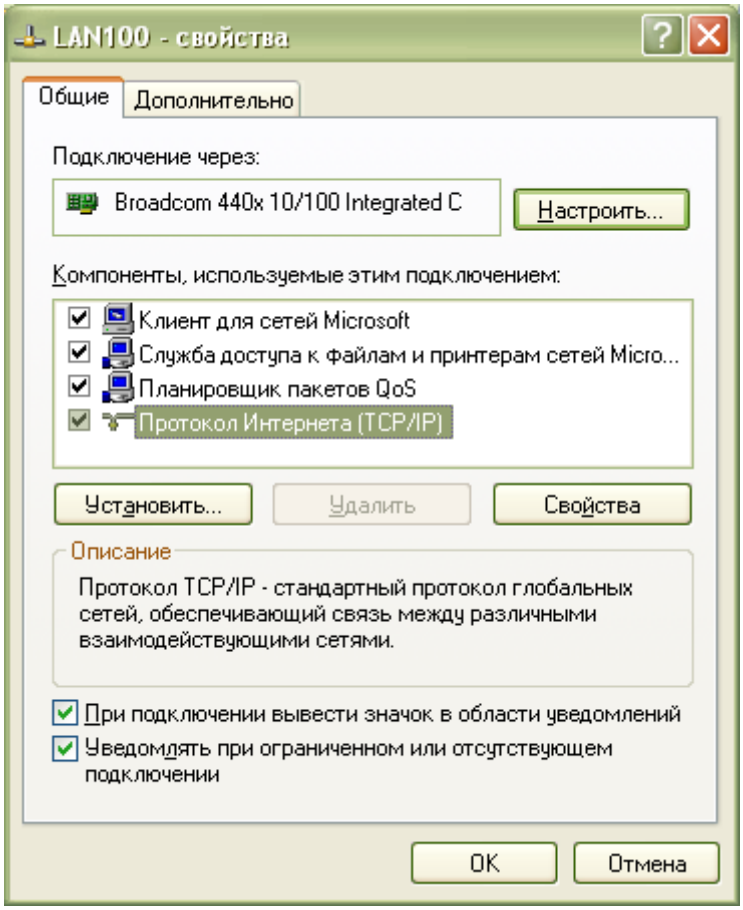


Рис. 3.2. Выбор протокола TCP/IP для настройки

После выбора Протокол Интернета (TCP/IP) производится настройка основных параметров TCP/IP. Для успешной работы в сети сетевому интерфейсу должен быть назначен уникальный IP-адрес и маска подсети. В случае, если планируется выход за пределы сети (например, в Интернет), указывается основной шлюз. А для того, чтобы браузер компьютера определял IP-адреса хостов по доменным именам в Интернете, указывается DNS-сервер (рис. 3.3).

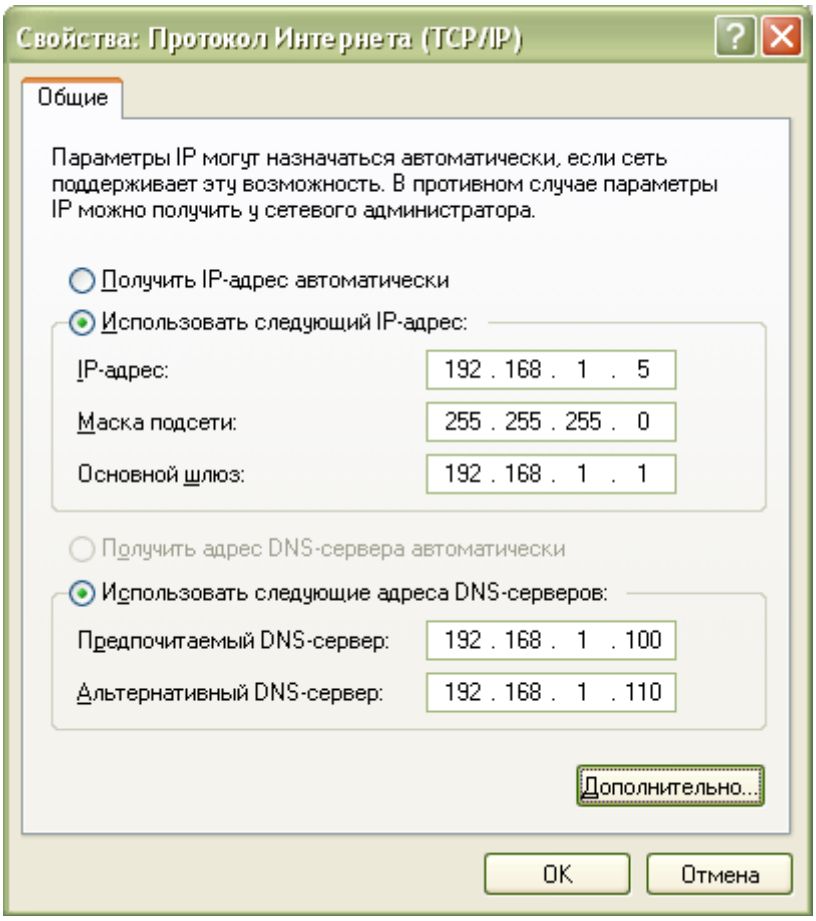


Рис. 3.3. Настройка основных параметров TCP/IP

IP-адрес и другие параметры могут быть настроены вручную (статический IP), получены от DHCP-сервера, выполняющего роль сервера, раздающего хостам сетевые настройки (динамический IP) или сконфигурированы по протоколу APIPA (автосконфигурированный IP).

В дополнительных параметрах TCP/IP имеется возможность произвести дополнительную настройку основных сетевых параметров (рис. 3.4).

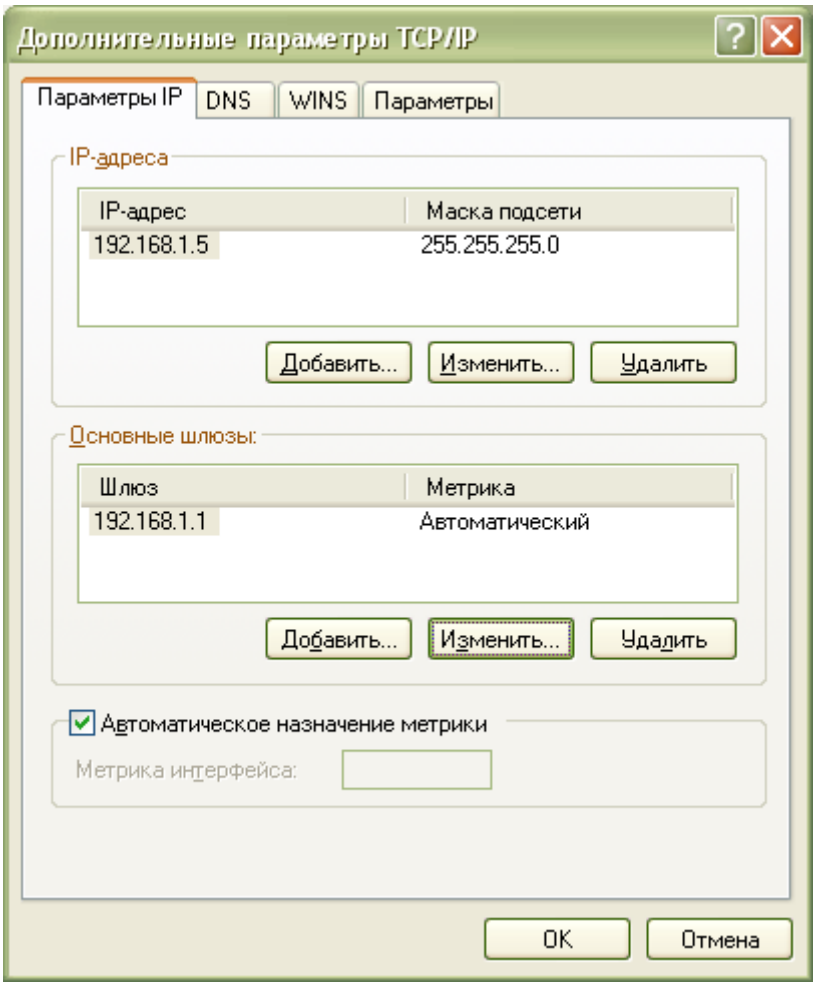


Рис. 3.4. Дополнительные параметры TCP/IP

Так, например, можно добавить второй IP-адрес из другой сети, что в дальнейшем позволит хосту обмениваться пакетами с хостами не только первой, но и второй сети.

Метрика, как правило, задается автоматически по-умолчанию. Данный параметр отвечает за выбор маршрута в сети. Фактически, метрика – это число переходов пакета до места назначения. Отметим, что все хосты локальной сети до маршрутизатора считаются равноудаленными друг от друга, а маршрутизатор, используемый на пути к хосту-получателю, является дополнительным устройством, которое увеличивает маршрут. Таким образом, метрика используется для определения наилучшего маршрута, ее значение определяет приоритет, который назначается маршруту, связанному с определенным интерфейсом. Чем меньше значение метрики, тем выше приоритет.

Просмотр сетевых параметров в ОС Windows NT осуществляется при помощи утилиты **ipconfig**, которая выводит информацию о настроенных сетевых интерфейсах (рис. 3.5).

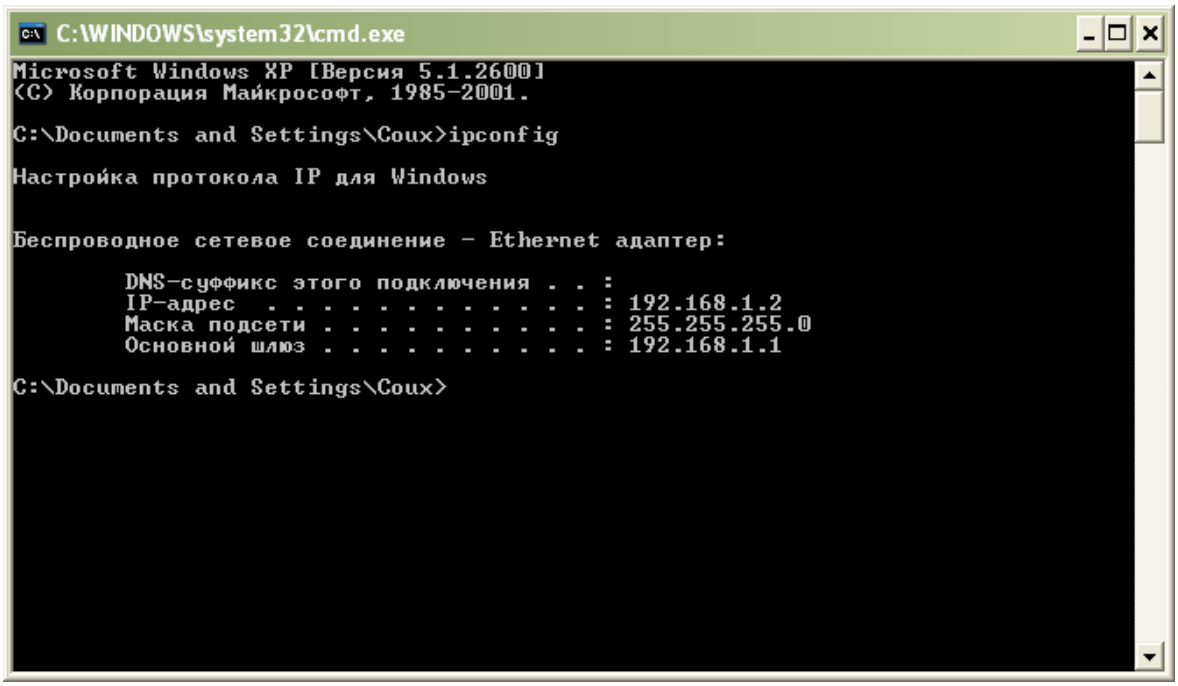


Рис. 3.5. Просмотр сетевых параметров в ОС Windows NT

Особое внимание при настройке сетевых параметров необходимо уделить специальному префиксу – маске подсети (Subnet Mask), так как именно она определяет, какая часть IP-адреса хоста относится к адресу сети, а какая – к адресу самого узла в этой сети. Маска подсети определяет, к какому классу адресов относится IP-адрес хоста, а также задает расширение префикса.

Таким образом, маска подсети обеспечивает выделение сетевого спектра с заданным расширением, что обеспечивает рациональное использование адресного пространства и снижает рост таблиц маршрутизации в Интернете. Она представляет собой 32-разрядное двоичное число, в разрядах расширенного префикса которого содержатся единицы, в остальных разрядах присутствуют нули.

На практике упрощенная запись IP-адреса/маски (CIDR-нотация) представляет собой вид: [IP-адрес]/[длина расширенного префикса]. Например, запись 192.168.0.1/24 (24 – число единиц в маске подсети) говорит, о том, что мы имеем дело с маской 255.255.255.0.

Согласно документам RFC 990 и RFC 997 существует 5 классов IP-адресов, для которых описано количество бит в IP-адресе, которое отводится для номера сети и номера хоста. Также для специальных целей выделены служебные IP-адреса, они зарезервированы и не могут быть использованы для обычных целей.

3.5. Служебные IP-адреса

При работе с сетевыми устройствами, настройке сетевых интерфейсов, анализе статистики сетевого трафика необходимо учесть следующие правила распределения IP-адресов.

- Если все биты IP-адреса устройства равны 0, то это адрес данного устройства.
- Если поле номера сети состоит из нулей, то получатель IP-пакета принадлежит той же самой сети, что и отправитель.
- Если все биты IP-адреса равны 1, то IP-пакет с таким адресом должен рассылаться всем хостам, находящимся в той же сети, что и его отправитель. Такая рассылка называется ограниченным широковещательным сообщением (Limited Broadcast).
- Если первый байт адреса равен 127, то адрес обозначает тот же самый узел. Такой адрес используется для взаимодействия процессов на одной и той же машине (например, для тестирования прикладных программ). Этот адрес имеет название возвратного (Loopback) и соответствует сетевому имени хоста localhost, которое воспринимается только самим хостом.
- Если все биты номера хоста равны 0, то IP-пакет предназначен для данной сети.
- Если все биты в поле номера хоста равны 1, то IP-пакет рассылается всем хостам сети с данным номером сети. Такая рассылка называется широковещательным сообщением (Broadcast).

Два последних пункта говорят о том, что в любой сети изначально имеется два зарезервированных IP-адреса: адрес сети и широковещательный адрес. Поэтому при расчете количества возможных хостов в сети от общего числа всегда отнимают эти два адреса.

3.6. Классы IP - адресов

Как было сказано выше, IP-адреса разделяются на 5 классов: A, B, C, D и E. Адреса классов A, B и C делятся на две логические части: номер сети и номер хоста. Идентификатор сети – адрес сети, который обозначает один сетевой сегмент в более крупной объединенной сети, где используется протокол TCP/IP. Таким образом, IP-адреса всех хостов в рамках одной сети имеют одинаковый идентификатор сети, который используется для уникального обозначения каждой сети в более крупной объединенной сети.

Идентификатор хоста, в свою очередь, являющийся его уникальным адресом, однозначно определяет узел TCP/IP в рамках своей сети. В качестве узла может выступать устройство, имеющее сетевой интерфейс: рабочая станция, сервер, коммутатор, маршрутизатор, сетевой принтер, и другие устройства, поддерживающие протокол TCP/IP. Возможен вариант, ко-

гда двум разным сетевым интерфейсам в одной сети назначается один IP-адрес. В этом случае произойдет так называемый конфликт IP-адресов, который повлечет за собой некорректную работу этих узлов в сети.

Класс A

У адресов класса A старший бит равен 0. Длина сетевого префикса составляет 8 бит (1 байт). Под номер узла выделяется 24 бита (3 байта). Таким образом, класс A может содержать 2^7–2=126 сетей. Каждая сеть этого класса может поддерживать максимум 2^{24}–2=16777214 узлов (рис. 3.6).

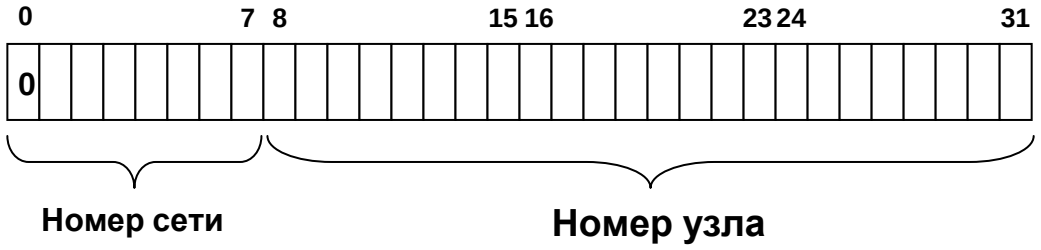


Рис. 3.6. Класс A

Очевидно, что адреса класса A предназначены для использования в больших сетях, с большим количеством узлов. На сегодняшний день в Интернете все адреса класса A распределены.

Класс B

У адресов класса B два старших бита равны 1 и 0 соответственно. Длина сетевого префикса и поле номера узла составляют 16 бит (2 байта). Таким образом, класс B может содержать 2^{14}=16384 сетей. Каждая сеть этого класса может поддерживать до 2^{16}–2=65534 узлов (рис. 3.7).

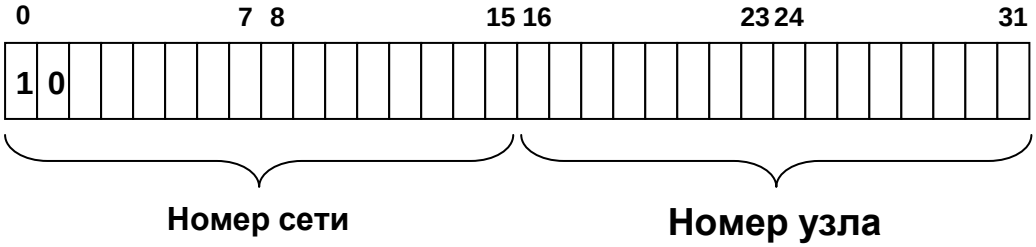


Рис. 3.7. Класс B

Класс B предназначен для применения в сетях среднего размера – уровень крупного предприятия.

Класс C

У адресов класса C три старших бита равны 1, 1 и 0 соответственно. Длина сетевого префикса составляет 24 бита (3 байта), номер узла занимает 8 бит (1 байт). Максимально возможное количество сетей класса C составляет 2^{21}=2097152. Каждая сеть может поддерживать до 2^8–2=254 узлов (рис. 3.8).

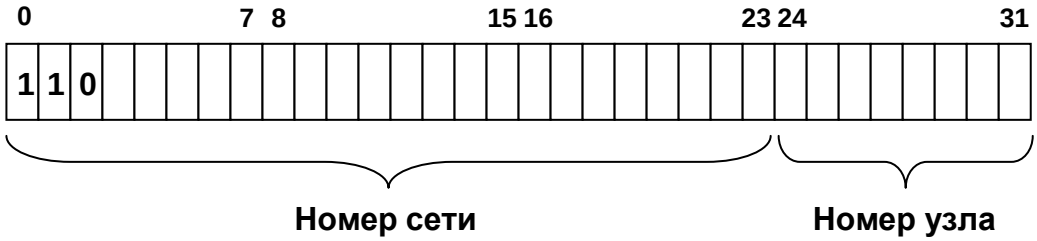


Рис. 3.8. Класс C

Очевидно, класс C предназначен для сетей с небольшим количеством узлов.

Класс D

Адреса класса D представляют собой специальные адреса, которые не относятся к отдельным сетям. В них отсутствует сетевой префикс, для них не определяются номера сетей. Каждый узел сети класса D имеет уникальный номер. Первые 4 бита адреса класса D равны 1110. Таким образом, значение первого октета этого диапазона адресов находится в пределах от 224 до 239. То есть диапазон используемых адресов выглядит следующим образом: 224.0.0.0 – 239.255.255.255 (рис. 3.9).

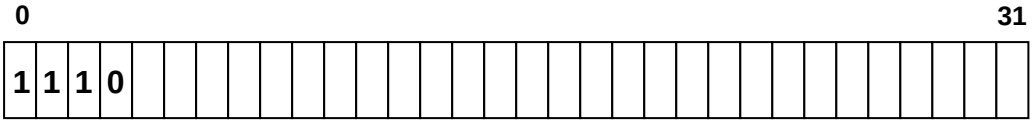


Рис. 3.9. Класс D

Адреса класса D используются для рассылки многоадресных пакетов, то есть предназначенных многочисленным группам хостов. Трафик, передаваемый по правилу многоадресной рассылки, называется multicast-трафиком. Для регулирования multicast-трафика был разработан межсетевой протокол управления multicast-группами IGMP (Internet Group Management Protocol).

Класс E

Адреса диапазона 240.0.0.0 – 255.255.255.255 относятся к классу E. Первый байт этих адресов содержит вначале биты 1111 (рис. 3.10).

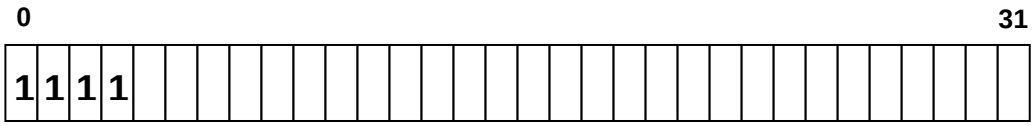


Рис. 3.10. Класс E

Данные адреса были зарезервированы для будущих дополнений в схеме адресации IP, но перспектива их использования сегодня находится под вопросом, так как существует более новая версия IP – протокол IPv6.
Приведем сводную таблицу по рассмотренным классам IP адресов (табл. 3.1).

Таблица 3.1

Класс	Старшие биты	Диапазоны адресов	Максимальное количество	
			сетей	узлов
A	0	1.0.0.0 – 126.0.0.0	$2^7 - 2$	$2^{24} - 2$
B	10	128.0.0.0 – 191.255.0.0	2^{14}	$2^{16} - 2$
C	110	192.0.0.0 – 223.255.255.255	2^{21}	$2^8 - 2$
D	1110	224.0.0.0 – 239.255.255.255	-	-
E	1111	240.0.0.0 – 254.255.255.255	-	-

3.7. Распределение IP-адресов в частных локальных сетях

В документах RFC 1918 и RFC 3330 определены диапазоны IP-адресов и их назначение. Так для организации частной локальной сети рекомендуется использование IP-адресов из трех возможных диапазонов (табл. 3.2).

Таблица 3.2

Диапазон адресов	Кол-во сетей	Класс адресов
10.0.0.0/8 – 10.255.255.255/8	1	A
172.16.0.0/12 – 172.31.255.255/12	16	B
192.168.0.0/16 – 192.168.255.255/16	256	C

IP-адреса, входящие в данные диапазоны, не значатся в таблицах глобальной маршрутизации Интернет. Любой может использовать IP-адреса из этих диапазонов без согласования с IANA или Интернет-провайдерами. В результате, эти адреса в настоящее время используются во множестве частных локальных сетей. Таким образом, уникальность адресов сохраняется

только в масштабе одной или нескольких сетей, которые согласованно используют общий блок адресов.

Публичные адреса для связи узлов частной сети с внешними сетями следует получать через провайдеров Интернет. Такие адреса не могут входить ни в один из указанных выше диапазонов частных адресов.

Поскольку частные адреса не имеют глобального значения, маршрутная информация о частных сетях не будет выходить за пределы этих сетей, а пакеты с частными адресами отправителей или получателей не будут передаваться через маршрутизаторы провайдеров Интернет.

Приведем пример использования IP-адресов в частной локальной вычислительной сети для обеспечения связью десяти рабочих станций. В качестве диапазона будем использовать сеть 172.17.117.0/28. Такая сеть должна обеспечить IP-адресами 2^4–2=14 узлов. Один адрес – адрес сети, еще один адрес – широковещательный. Для наглядности распределения IP-адресов приведем таблицу (табл. 3.3).

Таблица 3.3

Узлы	IP-адрес (CIDR)	IP-адрес (двоичный)
Сеть	172.17.117.0/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0000**
Хост1	172.17.117.1/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0001**
Хост2	172.17.117.2/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0010**
Хост3	172.17.117.3/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0011**
Хост4	172.17.117.4/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0100**
Хост5	172.17.117.5/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0101**
Хост6	172.17.117.6/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0110**
Хост7	172.17.117.7/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **0111**
Хост8	172.17.117.8/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1000**
Хост9	172.17.117.9/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1001**
Хост10	172.17.117.10/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1010**
Резерв	172.17.117.11/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1011**
Резерв	172.17.117.12/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1100**
Резерв	172.17.117.13/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1101**
Резерв	172.17.117.14/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1110**
Широковещательный	172.17.117.15/28	1010 1100 . 0001 0001. 0111 0101 . 0000 **1111**

Из табл. 3.3 видно, что для обеспечения 10 узлов частной сети, оказалось достаточным использование сети 172.17.117.0/28. При этом сохранился резерв для подключения четырех узлов. Пятый дополнительный хост потребовал бы расширения адресного пространства, например, до сети 172.17.117.0/27, которая, в свою очередь, способна обеспечить IP-адресами уже 2^5–2=30 узлов.

3.8. Протокол ARP

Все узлы сети имеют сетевые интерфейсы, которые обладают уникальными физическими Ethernet-адресами, заданными на аппаратном

уровне – MAC-адресами. Можно сказать, что MAC-адреса являются физическими сетевыми адресами и используются для непосредственной связи между сетевыми интерфейсами узлов, расположенных в одном сегменте сети. IP-адреса, в свою очередь, носят логических характер, и могут принадлежать узлам, расположенным в совершенно разных сегментах, которые связаны между собой через цепочку различных коммутаторов и маршрутизаторов. Таким образом, неизбежно возникает задача преобразования IP-адресов в MAC-адреса. Эту задачу призван решать протокол ARP.

ARP (Address Resolution Protocol) – протокол канального уровня, предназначенный для определения MAC-адреса узла по известному его IP-адресу. Изначально данный протокол был спроектирован для сетей Ethernet, но принципы, заложенные в ARP, позволяют использовать его и для других типов сетей. Подробное описание протокола ARP приведено в документе RFC 826.

Принцип работы протокола ARP состоит в обмене между узлом-отправителем и узлом-получателем специальными сообщениями: ARP request (ARP-запрос) и ARP reply (ARP-ответ). Полученная в результате ARP-ответа информация (MAC-адрес, соответствующий указанному в ARP-запросе IP-адресу) помещается в специальную ARP-таблицу узла и хранится там определенное время. Стандартное время хранения записи в ARP-таблице составляет 2 минуты. Если данная запись не используется сетевым интерфейсом, то через две минуты она удаляется.

Узел может использовать записи ARP-таблицы для экономии времени определения искомого MAC-адреса узла, которому требуется передавать IP-пакеты.

Просмотр ARP-таблицы в операционной системе Windows NT может быть осуществлен при помощи утилиты **arp** с ключом **-a** (рис. 3.11).

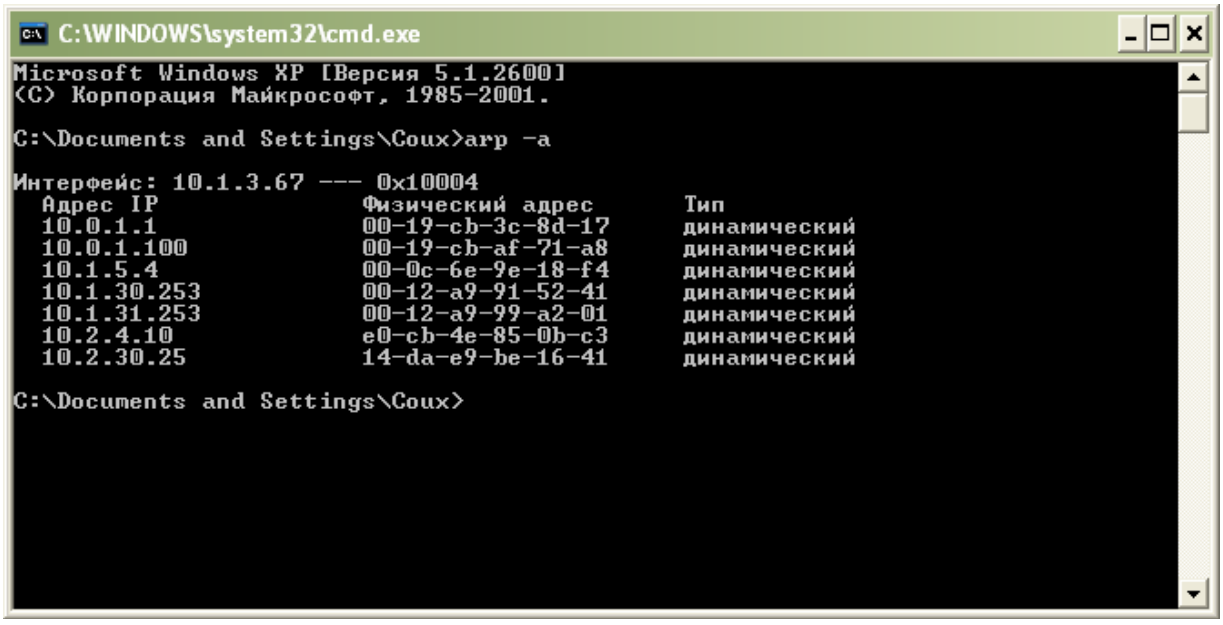


Рис. 3.11. Просмотр ARP-таблицы

Записи в ARP-таблице могут быть как динамическими (создаются при помощи ARP-запроса и ARP-ответа), так статическими (создаются в Windows NT при помощи команды утилиты **arp** с ключом **-s [IP-адрес] [MAC-адрес]**).

В случае отсутствия необходимой записи в ARP-таблице, узел-отправитель посылает ARP-запрос всем узлам, которые находятся в его сети, и получает ARP-ответ от нужного узла. Физически ARP-запрос представляет собой широковещательную рассылку кадров Ethernet. Кадр ARP-запроса состоит из заголовка кадра и непосредственно ARP-сообщения, помещенного в поле данных (рис. 3.12).

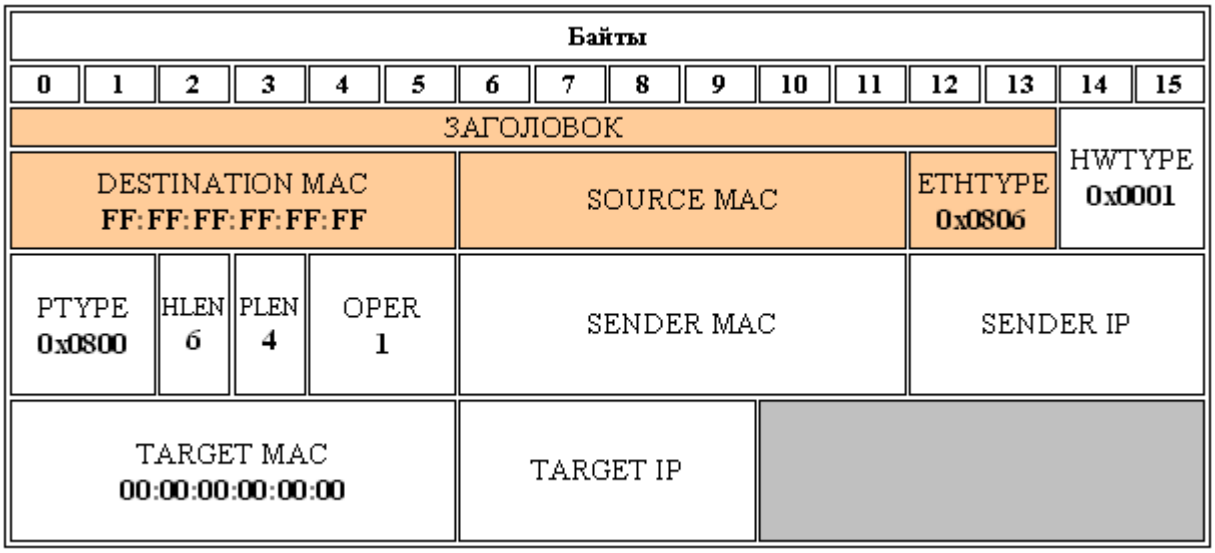


Рис. 3.12. Кадр ARP-запроса

- DESTINATION MAC – физический адрес узла-получателя кадра Ethernet. При широковещательной рассылке его значение равно FF:FF:FF:FF:FF:FF.
- SOURCE MAC – физический адрес узла-отправителя кадра Ethernet.
- ETHTYPE – тип кадра Ethernet. Если кадр несет ARP-сообщение, то это значение равно 0x0806 (в шестнадцатеричной системе счисления).
- HWTYPE – тип оборудования, работающего с канальным протоколом передачи данных. Для Ethernet это значение равно 0x0001 (в шестнадцатиричной системе счисления).
- PTYPE – тип протокола, который используется узлом-отправителем на более высоком уровне. Так как выше Ethernet располагается протокол IPv4, данное значение равно 0x0800 (в шестнадцатеричной системе счисления).
- HLEN – длина физического адреса в байтах. В данном случае используются MAC-адреса длиной 6 байт.

- PLEN – длина IP-адреса в байтах. При использовании протокола IPv4 данное значение равно 4.
- OPER – код операции ARP-сообщения (1 – запрос, 2 – ответ).
- SENDER MAC – физический адрес узла-отправителя информации.
- SENDER IP – IP-адрес узла-отправителя информации.
- TARGET MAC – физический адрес узла-получателя информации. При ARP-запросе данный параметр неизвестен, поэтому его значение устанавливается, как 00:00:00:00:00:00.
- TARGET IP – IP-адрес узла-получателя информации.

Все узлы локальной сети получают данный кадр (рис. 3.12), определяют по заголовку (поле ETHTYPE), что он несет в себе ARP-сообщение, и анализируют его содержимое. Поле OPER, значение которого равно 1, говорит узлам о том, что это ARP-запрос, на который они должны ответить или проигнорировать его.

Каждый узел, получивший ARP-запрос, производит сравнение собственного IP-адреса с адресом, указанным в поле TARGET IP (рис. 3.12). Если среди всех узлов найдется узел, IP-адрес которого является искомым, то он формирует кадр ARP-ответа, в котором заполняет поле TARGET MAC, указывая свой физический адрес. Также при ARP-ответе меняются местами пары адресов отправителя и получателя, значение поля OPER устанавливается равным 2 (рис. 3.13).

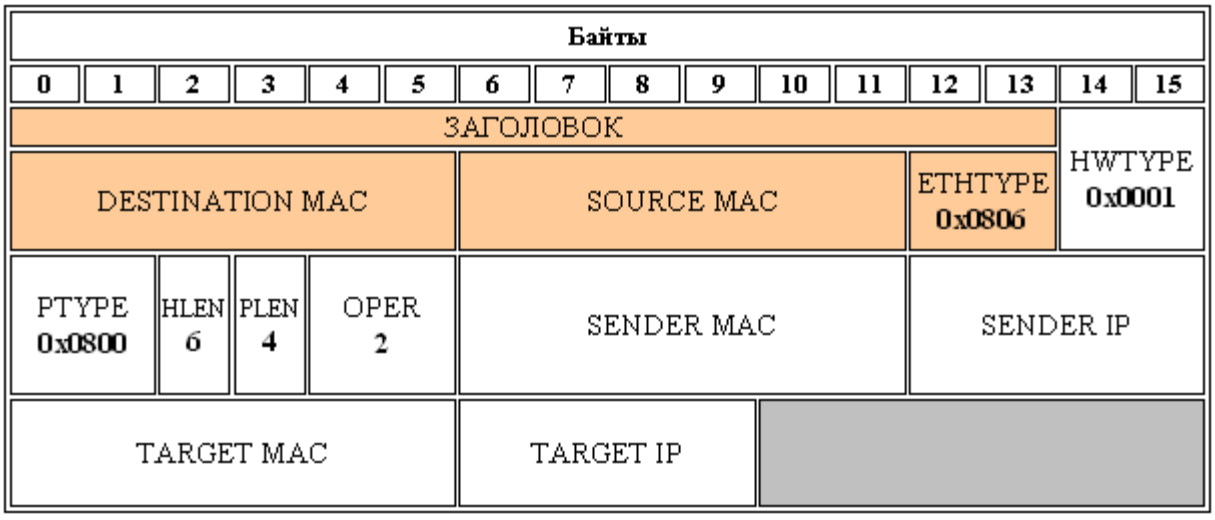


Рис. 3.13. Кадр ARP-ответа

- DESTINATION MAC – физический адрес узла-получателя ARP-ответа (узел-отправитель ARP-запроса).
- SOURCE MAC – физический адрес узла-отправителя кадра Ethernet (узел-отправитель ARP-ответа).
- OPER – код операции ARP-сообщения (1 – запрос, 2 – ответ).

- SENDER MAC – физический адрес узла-получателя информации (узел-отправитель ARP-ответа).
- SENDER IP – IP-адрес узла-получателя информации (узел-отправитель ARP-ответа).
- TARGET MAC – физический адрес узла-отправителя информации (узел-отправитель ARP-запроса).
- TARGET IP – IP-адрес узла-отправителя информации (узел-отправитель ARP-запроса).

После того, как узел-отправитель ARP-запроса (отправитель информации) получает ARP-ответ, определяется MAC-адрес узла-получателя информации и вместе с соответствующим IP-адресом заносится в ARP-таблицу узла-отправителя информации.

Обратившись к своей ARP-таблице, узел-отправитель IP-пакетов устанавливает по IP-адресу узла-получателя его MAC-адрес. После этого узел-отправитель информации формирует из IP-пакетов кадры Ethernet и отправляет их на соответствующий сетевой интерфейс узла-получателя информации.

Схема обмена информацией двух хостов в рамках одной локальной сети показана на рис. 3.14. Данный пример демонстрирует передачу кадра Ethernet от сетевого интерфейса одного компьютера на сетевой интерфейс другого в случае отсутствия записи в ARP-таблице. При этом кадры ARP-запроса и ARP-ответа будут иметь следующий вид (рис. 3.15 и рис. 3.16).

В заключение можно добавить, что передача кадров ARP-сообщений и кадров с информацией осуществляется через коммутатор (рис. 3.14), который также обладает MAC-адресом (один на все сетевые интерфейсы) и даже IP-адресом (если это управляемый коммутатор). Но данные сетевые параметры используются только для управления коммутатором.

Обновляя таблицу соответствия MAC-адресов устройств, подключенных к его физическим портам, коммутатор сам является прозрачным сетевым устройством и не принимает непосредственного вмешательства в процесс передачи пакетов.

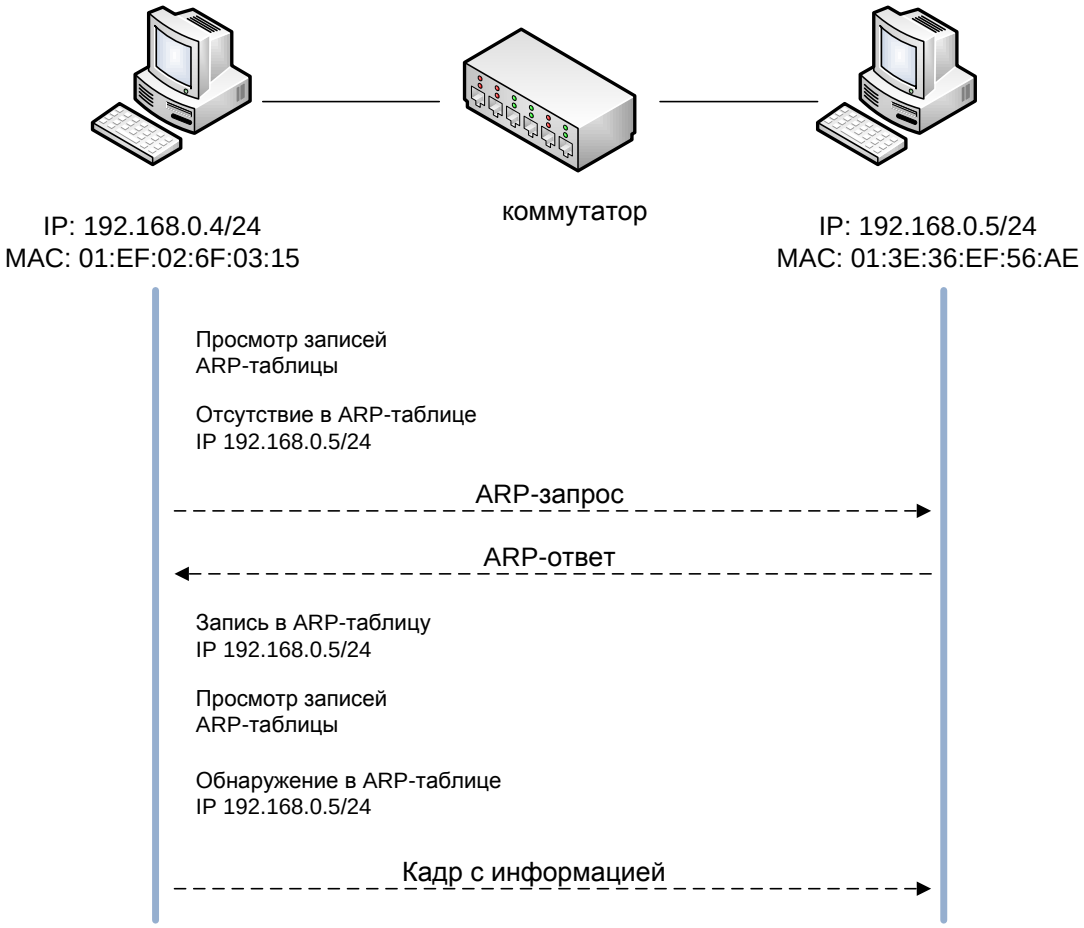


Рис. 3.14. Схема обмена информацией двух хостов в локальной сети

Байты														
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ЗАГОЛОВОК														0x0001	
FF:FF:FF:FF:FF:FF						01:EF:02:6F:03:15						0x0806			
0x0800		6		4		1		01:EF:02:6F:03:15				192.168.0.4			
00:00:00:00:00:00						192.168.0.5									

Рис. 3.15. Пример кадра ARP-запроса

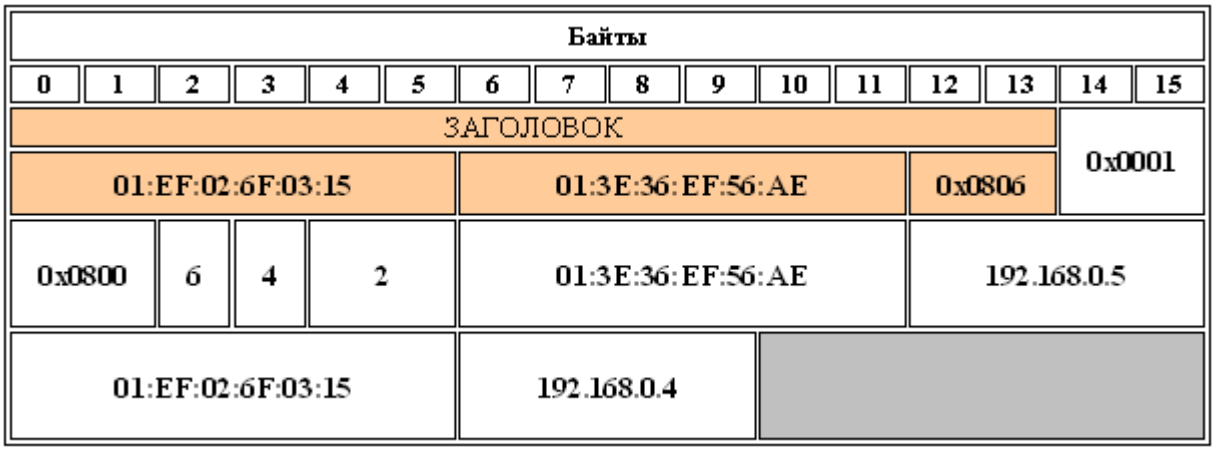


Рис. 3.16. Пример кадра ARP-ответа

3.9. Маршрутизация

Современные сети передачи данных, призванные решать серьезные задачи, строятся на основе нескольких (и даже множества) контуров. То есть каждая сеть зачастую является подсетью, входящей в сеть более высокого порядка. Такое построение сетей позволяет не только сэкономить адресное пространство, но и обеспечить оптимальное распределение трафика внутри всей сетевой инфраструктуры.

Вопрос объединения локальных вычислительных сетей, имеющих собственные адресные пространства, требует решения двух основных задач: определение оптимального маршрута между узлом-отправителем и узлом-получателем информации, и непосредственно их коммутация.

Коммутация в рамках одного сегмента осуществляется коммутатором L2 (второго уровня), который определяет, в какой порт отправлять кадры на основании таблицы MAC-адресов. Если же узел-получатель информации находится в другом сегменте, то пакету требуется преодолеть шлюз и перейти из одного сегмента сети в другой. Выполнение данной процедуры обеспечивается маршрутизатором – коммутатором L3 (третьего уровня) с функцией маршрутизации.

Алгоритмы маршрутизации определяют показатели маршрута и позволяют найти оптимальный путь следования пакетов от узла-отправителя до узла-получателя. Процесс обнаружения маршрута основан на использовании таблиц маршрутизации, в которых содержится маршрутная информация.

Просмотр таблицы маршрутизации в ОС Windows NT может быть осуществлен при помощи утилиты **route** с параметром **print** (рис. 3.17).

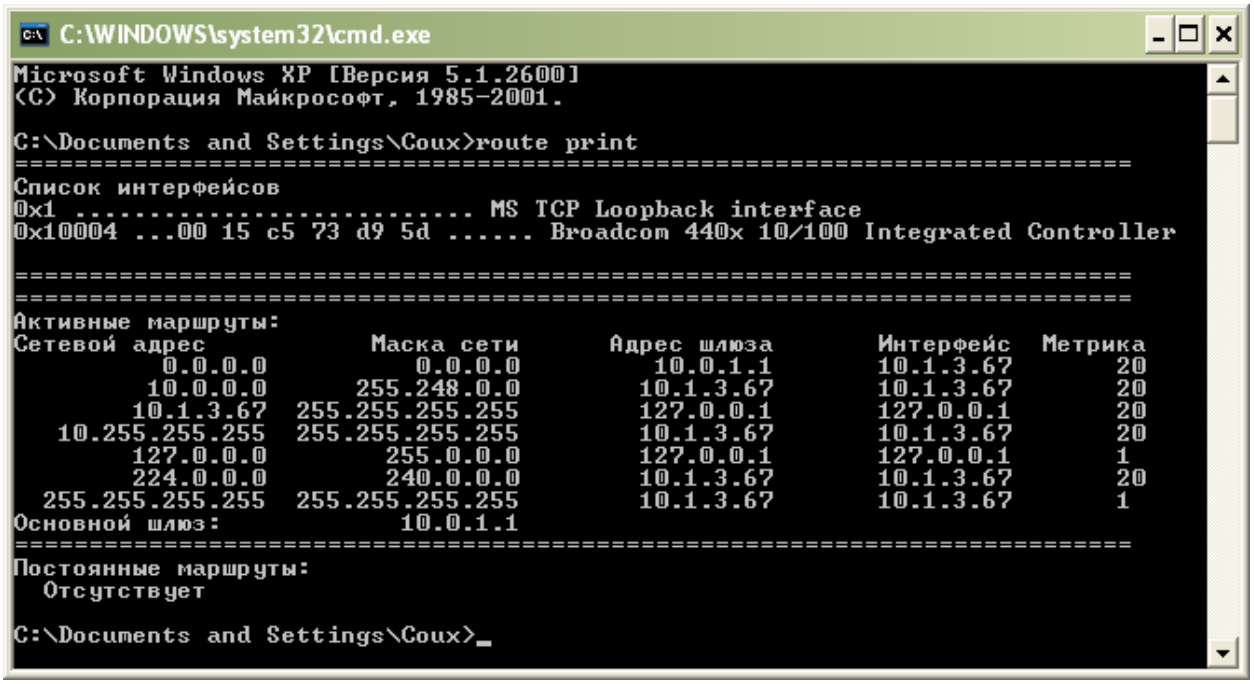


Рис. 3.17. Таблица маршрутизации в ОС Windows NT

Маршрутная информация в таблицах маршрутизации изменяется в зависимости от используемого алгоритма маршрутизации. Однако для определения оптимального маршрута в любой таблице маршрутизации должны содержаться следующие данные о маршрутах:

- сеть назначения (IP-адрес и маска подсети);
- следующий шаг в направлении сети назначения;
- сетевой интерфейс, который будет использоваться для передачи;
- стоимость (метрика) маршрута.

На основании этих данных появится возможность определить сетевой адрес узла-получателя пакета и сетевой интерфейс, который при этом будет использован.

Использование записей таблицы маршрутизации происходит в том случае, если узел-отправитель пакетов не может найти по IP-адресу в локальной сети узел-получателя. Таким образом, делается вывод о том, что узел-получатель расположен в другой сети.

Для передачи пакетов в другую сеть узел-отправитель обращается к своей таблице маршрутизации и выполняет ряд шагов:

1. Для каждого маршрута вычисляется побитовое «И» поля «Маска подсети» и IP-адреса получателя. Маршруты, для которых результат совпадает со значением поля «Адрес сети назначения», считаются подходящими.
2. Если маршрутов, отобранных на шаге 1, несколько, из них выбираются маршруты с максимальным количеством единиц в маске подсети.

3. Если маршрутов, отобранных на шаге 2, несколько, из них выбираются маршруты с максимальной метрикой.
4. Если маршрутов, отобранных на шаге 3, несколько, из них выбирается произвольный маршрут.

Если на шаге 1 подходящих маршрутов обнаружено не было, узел-отправитель использует адрес шлюза по умолчанию для доставки пакета к маршрутизатору. Маршрутизатор определяет маршрут к узлу-получателю в своей таблице маршрутизации. Если маршрут снова не будет найден, пакет посылается по адресу шлюза, заданного по умолчанию в таблице маршрутизатора.

Стандартная Таблица маршрутизации содержит:

- автоматически генерируемые маршруты – маршруты, сформированные на основании параметров данного узла;
- статические маршруты – маршруты, сформированные в результате выполнения специальных команд;
- динамические маршруты – маршруты, сформированные на основании информации, которой маршрутизаторы обмениваются между собой согласно специальным протоколам маршрутизации.

3.9.1. Автоматически генерируемые маршруты

Автоматически генерируемые маршруты создаются, как правило, операционной системой узла на основании имеющихся параметров сетевого подключения: IP-адрес сетевого интерфейса, маска подсети, шлюз по умолчанию.

Рассмотрим пример построения автоматически генерируемых маршрутов в таблице маршрутизации в ОС Windows NT. Настроим сетевой интерфейс следующим образом:

- IP-address: 192.168.1.5
- Маска подсети: 255.255.255.0
- Шлюз по умолчанию: 192.168.1.1

В результате Таблица маршрутизации будет дополнена следующими записями.

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.5	1

Маршрут по умолчанию.

Значения полей

- Сеть назначения: 0.0.0.0
- Маска подсети: 0.0.0.0
- Следующий шаг: IP-адрес шлюза по умолчанию
- Интерфейс: IP-адрес сетевого интерфейса, подключенного к той же сети, к которой подключен шлюз по умолчанию

Является подходящим для любого IP-адреса получателя
Присутствует только, если задан шлюз по умолчанию

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1

Маршрут для петлевых адресов.
Значения полей

- Сеть назначения: 127.0.0.0
- Маска подсети: 255.0.0.0
- Следующий шаг: 127.0.0.1
- Интерфейс: 127.0.0.1

Сетевая подсистема поддерживает специальный «петлевой» сетевой интерфейс (loopback). Кадр, отправленный через данный интерфейс, считается немедленно полученным от самого себя. Петлевому интерфейсу назначается IP-адрес 127.0.0.1

Маршрут для петлевых адресов является подходящим для адресов получателя 127.x.x.x и передает все пакеты, отправленные на данные адреса, через петлевой интерфейс

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
192.168.1.0	255.255.255.0	192.168.1.5	192.168.1.5	1

Маршрут в непосредственно подключенную сеть.
Значения полей

- Сеть назначения: адрес непосредственно подключенной сети
- Маска подсети: маска непосредственно подключенной сети
- Следующий шаг: IP-адрес подключенного к данной сети интерфейса
- Интерфейс: IP-адрес подключенного к данной сети интерфейса

Обеспечивает для данного узла непосредственную передачу пакета к узлу-получателю

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
192.168.1.5	255.255.255.255	127.0.0.1	127.0.0.1	1

Маршрут к локальному хосту.
Значения полей

- Сеть назначения: адрес данного узла
- Маска подсети: 255.255.255.255 (данный маршрут является подходящим только для одного IP-адреса получателя, который в точности совпадает со значением поля «Адрес сети»)
- Следующий шаг: 127.0.0.1
- Интерфейс: 127.0.0.1

Все пакеты, отправленные на локальный адрес, доставляются через петлевой интерфейс

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
192.168.1.255	255.255.255.255	192.168.1.5	192.168.1.5	1

Маршрут широковещательной рассылки в непосредственно подключенной сети.

Значения полей

- Сеть назначения: адрес широковещательной рассылки
- Маска подсети: 255.255.255.255
- Следующий шаг: IP-адрес подключенного к данной сети интерфейса
- Интерфейс: IP-адрес подключенного к данной сети интерфейса

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
224.0.0.0	224.0.0.0	192.168.1.5	192.168.1.5	1

Маршрут групповой рассылки.

Значения полей

- Сеть назначения: 224.0.0.0
- Маска подсети: 240.0.0.0
- Следующий шаг: IP-адрес сетевого интерфейса
- Интерфейс: IP-адрес сетевого интерфейса

Сеть назначения	Маска подсети	Следующий шаг	Интерфейс	Метрика
255.255.255.255	255.255.255.255	192.168.1.5	192.168.1.5	1

Маршрут ограниченной широковещательной рассылки.

Значения полей

- Сеть назначения: 255.255.255.255
- Маска подсети: 255.255.255.255
- Следующий шаг: IP-адрес сетевого интерфейса
- Интерфейс: IP-адрес сетевого интерфейса

Приведенные примеры маршрутов характерны для хоста под управлением ОС Windows. Они создаются автоматически при настройке параметров сетевого интерфейса. Маршрутизаторы, в свою очередь, требуют проведения более детальных настроек, так как должны обеспечивать передачу пакетов из одной сети в другую. При этом маршрутизаторы взаимодействуют друг с другом и могут даже обмениваться служебной информацией. Способ построения их таблиц маршрутизации зависит от используемых протоколов маршрутизации. В настоящее время выделяют два типа маршрутизации: статическую и динамическую.

3.9.2. Статическая маршрутизация

Статическая маршрутизация предполагает ручное построение и обновление таблиц маршрутизации. При изменении статического маршрута маршрутизатор не информирует об этом другие маршрутизаторы.

Рассмотрим построение таблиц со статическими маршрутами на примере объединения четырех подсетей через маршрутизаторы (рис. 3.18).

На рис. 3.18 использованы следующие обозначения:

- Маршрутизаторы – R_1, R_2, R_3, R_4
- Коммутаторы в подсетях – SW_1, SW_2, SW_3, SW_4
- Подсети верхнего контура – Net-R_{12}, Net-R_{13}, Net-R_{24}, Net-R_{34}
- Подсети нижнего контура – Net-SW_1, Net-SW_2, Net-SW_3, Net-SW_4

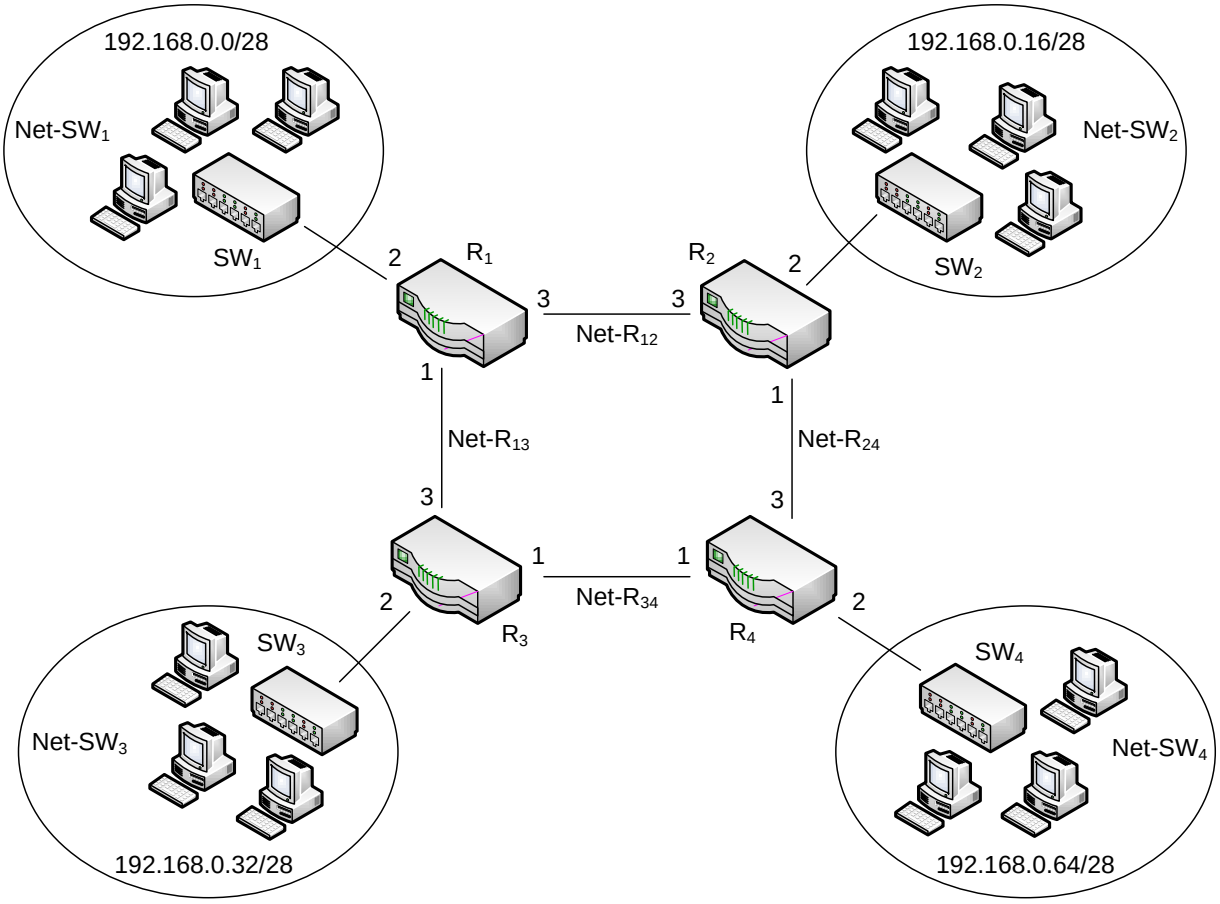


Рис. 3.18. Объединение четырех подсетей через маршрутизаторы

Перед построением таблиц маршрутизации необходимо произвести предварительную настройку сетевых устройств – присвоить IP-адреса интерфейсам маршрутизаторов в подсетях верхнего контура (табл. 3.4), а также выделить адреса для хостов, расположенных в подсетях нижнего контура, и указать для них шлюзы по умолчанию (табл. 3.5).

Таблица 3.4

Адресное пространство подсетей верхнего контура

Подсеть	IP-адрес	Назначение
Net-R_{12}	172.16.1.0/30	Адрес подсети
	255.255.255.252	Маска подсети
	172.16.1.1/30	R_1 , интерфейс 3
	172.16.1.2/30	R_2 , интерфейс 3
	172.16.1.3/30	Широковещательный адрес
Net-R_{13}	172.16.1.4/30	Адрес подсети
	255.255.255.252	Маска подсети
	172.16.1.5/30	R_1 , интерфейс 1
	172.16.1.6/30	R_3 , интерфейс 3
	172.16.1.7/30	Широковещательный адрес
Net-R_{24}	172.16.1.8/30	Адрес подсети
	255.255.255.252	Маска подсети
	172.16.1.9/30	R_2 , интерфейс 1
	172.16.1.10/30	R_4 , интерфейс 3
	172.16.1.11/30	Широковещательный адрес
Net-R_{34}	172.16.1.12/30	Адрес подсети
	255.255.255.252	Маска подсети
	172.16.1.13/30	R_3 , интерфейс 1
	172.16.1.14/30	R_4 , интерфейс 1
	172.16.1.15/30	Широковещательный адрес

Адресное пространство, выделенное для подсетей верхнего контура, в данном примере учитывает только связь между двумя интерфейсами маршрутизаторов, поэтому достаточной является маска 255.255.255.252.

Адресное пространство, выделенное для подсетей нижнего контура, в свою очередь, позволяет обеспечить адресами 13 хостов, включая один адрес для управления коммутатором L2. Один IP-адрес в каждой из этих подсетей присваивается интерфейсу маршрутизатора, выполняющего роль шлюза для хостов.

Таблица 3. 5

Адресное пространство подсетей нижнего контура

Подсеть	IP-адрес	Назначение
Net-SW_1	192.168.0.0/28	Адрес подсети
	255.255.255.240	Маска подсети
	192.168.0.1/28	Шлюз – R_1 , интерфейс 2
	192.168.0.2 – 192.168.0.14	Хосты
	192.168.0.15/28	Широковещательный адрес
Net-SW_2	192.168.0.16/28	Адрес подсети
	255.255.255.240	Маска подсети

	192.168.0.17/28	Шлюз – R_2 , интерфейс 2
	192.168.0.18 – 192.168.0.30	Хосты
	192.168.0.31/28	Широковещательный адрес
Net-SW_3	192.168.0.32/28	Адрес подсети
	255.255.255.240	Маска подсети
	192.168.0.33/28	Шлюз – R_3 , интерфейс 2
	192.168.0.34 – 192.168.0.62	Хосты
	192.168.0.63/28	Широковещательный адрес
Net-SW_4	192.168.0.64/28	Адрес подсети
	255.255.255.240	Маска подсети
	192.168.0.65/28	Шлюз – R_4 , интерфейс 2
	192.168.0.66 – 192.168.0.78	Хосты
	192.168.0.79/28	Широковещательный адрес

Учитывая схему соединения сетевых устройств (рис. 3.18), построим для маршрутизаторов таблицы маршрутизации, которые должны обеспечивать передачу данных между всеми узлами сети.

Таблицы маршрутизации заполним вручную, построив всевозможные маршруты следования пакетов, что может быть очень полезным при выходе из строя отдельных маршрутизаторов. В качестве метрики будем использовать показатель, учитывающий не только число промежуточных узлов от узла-отправителя до узла-получателя, но и приоритетность направления пути следования пакетов (табл. 3.6).

Таблица 3. 6

Информация о маршрутах узлов

Маршрутизатор	Сеть назначения/маска	Шлюз	Метрика
R_1	172.16.1.0/255.255.255.252	Прямое подключение	-
	172.16.1.4/255.255.255.252	Прямое подключение	-
	172.16.1.8/255.255.255.252	172.16.1.2	1
	172.16.1.8/255.255.255.252	172.16.1.6	2
	172.16.1.12/255.255.255.252	172.16.1.6	1
	172.16.1.12/255.255.255.252	172.16.1.2	2
	192.168.0.0/255.255.255.240	Прямое подключение	-
	192.168.0.16/255.255.255.240	172.16.1.2	1
	192.168.0.16/255.255.255.240	172.16.1.6	3
	192.168.0.32/255.255.255.240	172.16.1.6	1
	192.168.0.32/255.255.255.240	172.16.1.2	3
	192.168.0.64/255.255.255.240	172.16.1.2	2
	192.168.0.64/255.255.255.240	172.16.1.6	10
R_2	172.16.1.0/255.255.255.252	Прямое подключение	-
	172.16.1.8/255.255.255.252	Прямое подключение	-
	172.16.1.4/255.255.255.252	172.16.1.1	1
	172.16.1.4/255.255.255.252	172.16.1.10	2
	172.16.1.12/255.255.255.252	172.16.1.10	1

	172.16.1.12/255.255.255.252	172.16.1.1	2
	192.168.0.16/255.255.255.240	Прямое подключение	-
	192.168.0.0/255.255.255.240	172.16.1.1	1
	192.168.0.0/255.255.255.240	172.16.1.10	3
	192.168.0.64/255.255.255.240	172.16.1.10	1
	192.168.0.64/255.255.255.240	172.16.1.1	3
	192.168.0.32/255.255.255.240	172.16.1.1	2
	192.168.0.32/255.255.255.240	172.16.1.10	10
R_3	172.16.1.4/255.255.255.252	Прямое подключение	-
	172.16.1.12/255.255.255.252	Прямое подключение	-
	172.16.1.0/255.255.255.252	172.16.1.5	1
	172.16.1.0/255.255.255.252	172.16.1.14	2
	172.16.1.8/255.255.255.252	172.16.1.14	1
	172.16.1.8/255.255.255.252	172.16.1.5	2
	192.168.0.32/255.255.255.240	Прямое подключение	-
	192.168.0.0/255.255.255.240	172.16.1.5	1
	192.168.0.0/255.255.255.240	172.16.1.14	3
	192.168.0.64/255.255.255.240	172.16.1.14	1
	192.168.0.64/255.255.255.240	172.16.1.5	3
	192.168.0.16/255.255.255.240	172.16.1.5	2
	192.168.0.16/255.255.255.240	172.16.1.14	10
R_4	172.16.1.8/255.255.255.252	Прямое подключение	-
	172.16.1.12/255.255.255.252	Прямое подключение	-
	172.16.1.0/255.255.255.252	172.16.1.9	1
	172.16.1.0/255.255.255.252	172.16.1.13	2
	172.16.1.4/255.255.255.252	172.16.1.13	1
	172.16.1.4/255.255.255.252	172.16.1.9	2
	192.168.0.64/255.255.255.240	Прямое подключение	-
	192.168.0.16/255.255.255.240	172.16.1.9	1
	192.168.0.16/255.255.255.240	172.16.1.13	3
	192.168.0.32/255.255.255.240	172.16.1.13	1
	192.168.0.32/255.255.255.240	172.16.1.9	3
	192.168.0.0/255.255.255.240	172.16.1.9	2
	192.168.0.0/255.255.255.240	172.16.1.13	10

Динамическое построение маршрутов при включении, например, протокола маршрутизации RIP в значительной степени упростило бы и оптимизировало данные в табл. 3.6. Однако, применение статических маршрутов позволило жестко определить приоритеты путей следования трафика по сети, вручную указав для нужных маршрутов определенные значения метрики.

При этом необходимо отметить, что наличие в сети хотя бы одного статического маршрутизатора требует настройки записей статических таблиц маршрутизации для всех подсетей на каждом маршрутизаторе данной сети.

Рассмотрим пример использования статической маршрутизации в сети, где роль шлюзов выполняют компьютеры с несколькими сетевыми интерфейсами (рис. 3.19).

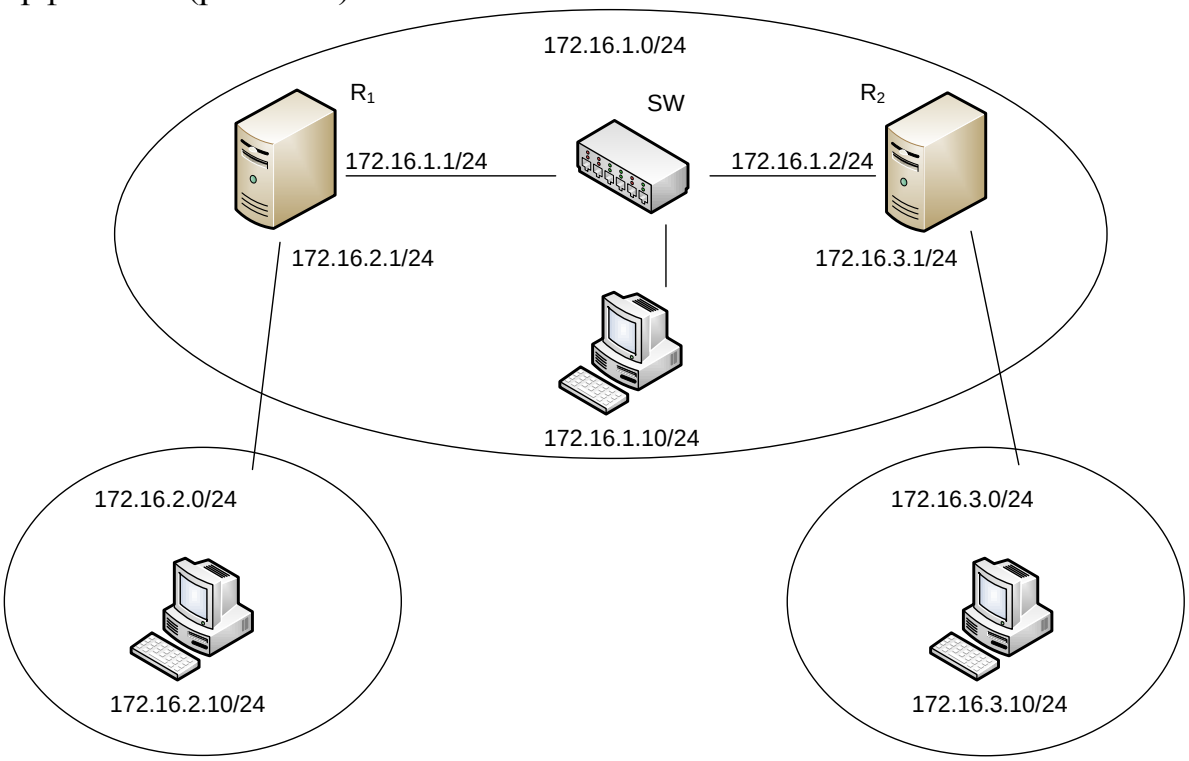


Рис. 3.19. Объединение подсетей при помощи компьютеров

Компьютер 172.16.2.10 обменивается данными с узлами своей сети 172.16.2.0 и имеет выход в сеть 172.16.1.0 через интерфейс компьютера-шлюза R_1 (172.16.2.1). Компьютер 172.16.3.10 кроме своей сети 172.16.3.0 также связан с сетью 172.16.1.0 через интерфейс компьютера-шлюза R_2 (172.16.3.1). При этом хосты сетей 172.16.1.0, 172.16.2.0, 172.16.3.0 не могут обмениваться информацией между собой, пока не будут добавлены соответствующие записи в таблицы маршрутизации R_1 и R_2.

Таблицы маршрутизации при такой настройке сети составлены статически и выглядят следующим образом (табл. 3.7).

Таблица 3.7

Информация о маршрутах узлов

Маршрутизатор	Сеть назначения/маска	Шлюз	Метрика
R_1	172.16.1.0/24	172.16.1.1	-
	172.16.2.0/24	172.16.2.1	-
	172.16.3.0/24	172.16.1.2	1
R_2	172.16.1.0/24	172.16.1.2	-
	172.16.3.0/24	172.16.3.1	-
	172.16.2.0/24	172.16.1.1	1

Третья запись статической таблицы маршрутизации на компьютере R_1 содержит в поле сети назначения адрес 172.16.3.0/24, а в качестве следующего узла – IP-адрес интерфейса компьютера-шлюза R_2 (172.16.1.2), к которому R_1 имеет прямой доступ, и который будет пересылать пакеты из сети 172.16.2.0 в сеть 172.16.3.0. При этом в качестве шлюза на компьютере 172.16.2.10 должен быть указан интерфейс R_1 (172.16.2.1).

Аналогичным образом настроена статическая таблица маршрутизации R_2. Третья запись R_2 содержит в поле сети назначения адрес 172.16.2.0/24. В качестве шлюза для нее указан IP-адрес интерфейса R_1 (172.16.1.1), который напрямую связан с R_2 и обеспечивает передачу пакетов из сети 172.16.3.0 в сеть 172.16.2.0. Очевидно, что шлюзом для компьютера 172.16.3.10 является интерфейс R_2 (172.16.3.1).

В качестве компьютеров-шлюзов с несколькими сетевыми интерфейсами могут быть использованы машины с операционными системами как Linux, так и Windows.

Работа с таблицей маршрутизации в ОС Windows производится при помощи утилиты **route** с набором ключей и параметров:

- route -p add [сеть] mask [маска подсети] [шлюз] [метрика] [интерфейс] – добавление постоянного маршрута, маршрут сохраняется в реестре операционной системы и записывается в таблицу маршрутизации после каждого включения компьютера;
- route add [сеть] mask [сетевая маска] [шлюз] [метрика] [интерфейс] – добавление временного маршрута, маршрут хранится только в оперативной памяти компьютера;
- route delete [сеть] [шлюз] – удаление маршрута;
- route change [сеть] [шлюз] – редактирование маршрута;
- route print – отображение таблицы маршрутизации;
- route -f – очистка таблицы маршрутизации.

Так, например, для добавления постоянных маршрутов в таблицу маршрутизации R_1 и R_2 (табл. 3.7), которые обеспечивают обмен данными между компьютерами 172.16.2.10 и 172.16.3.10, были выполнены команды:

для R_1: route -p add 172.16.3.0 mask 255.255.255.0 172.16.1.2
для R_2: route -p add 172.16.2.0 mask 255.255.255.0 172.16.1.1

Отличительной особенностью статической маршрутизации является то, что маршрутизаторы не производят между собой автоматического обмена информацией о маршрутах. Заполнение статической таблицы маршрутизации осуществляется вручную или при назначении шлюза по умолчанию.

3.9.3. Динамическая маршрутизация

Динамическая маршрутизация осуществляется такими протоколами, как RIP, EIGRP, OSPF, BGP. Данные протоколы маршрутизации обеспечивают периодический обмен информацией между маршрутизаторами. Таким образом, при изменении маршрута в таблице маршрутизации одного маршрутизатора остальные маршрутизаторы автоматически узнают об этом.

Динамические протоколы маршрутизации используются, как правило, в больших и сложных по структуре сетях, где не так просто построить статические таблицы маршрутизации. Изменение конфигурации сети в одном сегменте требует редактирования таблиц маршрутизации на всех маршрутизаторах, связанных с данным сегментом. Динамические протоколы маршрутизации позволяют эффективно решить данную задачу, обеспечив оперативное построение оптимальных маршрутов в таблицах маршрутизации.

В отличие от статической маршрутизации, где таблица маршрутизации управлялась вручную (как правило, при помощи утилиты **route**), динамическая маршрутизация предполагает наличие в ядре операционной системы маршрутизатора специальной службы, которая запущена постоянно и занимается периодическим редактированием таблицы маршрутизации. Данная служба, проводя анализ структуры сети, определяет оптимальные маршруты и добавляет их в таблицу маршрутизации. Исчезновение того или иного маршрута на пути следования пакетов влечет за собой автоматическое перестроение таблиц маршрутизации динамических маршрутизаторов. Определяются новые оптимальные маршруты, которые записываются вместо неработоспособных.

Глобальная сеть Интернет представляет собой множество автономных систем, в каждой из которых используется собственный протокол маршрутизации, обеспечивающий взаимодействие маршрутизаторов внутри своей сети.

Такие протоколы, которые обеспечивают маршрутизацию внутри автономной системы, относят к категории протоколов внутридоменной маршрутизации – IGP (Interior Gateway Protocol). Основные на сегодняшний день протоколы IGP – это RIP, EIGRP и OSPF.

Протоколы междоменной маршрутизации – EGP (Exterior Gateway Protocols), в свою очередь, предназначены для организации взаимодействия между маршрутизаторами, расположенными в разных автономных системах. Наиболее распространенным протоколом данной категории является BGP.

3.10. Протокол RIP

Протокол RIP (Routing Information Protocol) находит широкое применение в сетях, состоящих из сегментов с ограниченным адресным пространством. Речь идет о сетях, объединяющих территориально небольшие предприятия и офисы. Тем не менее, настройка статической маршрутизации в таких сетях, несмотря на скромные по меркам Интернет масштабы, является затруднительной.

Первая версия протокола RIP (RFC 1058) обладала рядом недостатков, среди которых основным было отсутствие поддержки масок переменной длины. То есть, RIPv1 не поддерживал бесклассовую маршрутизацию и обеспечивал только маршрутизацию подсетей с масками 255.0.0.0, 255.255.0.0 и 255.255.255.0.

Вторая версия протокола RIPv2 (RFC 2453) лишена данного недостатка. Также в ней реализовано вычисление метрики расстояния на основе критерия пропускной способности канала передачи данных. Но при этом, как и в предыдущей версии, в RIPv2 не поддерживается длина маршрута, превышающая 16 транзитных переходов. Необходимо также отметить, что обмен информацией в RIPv2 предполагает широковещательную рассылку маршрутизатором полной таблицы маршрутизации каждые 30 секунд, что, в некоторой степени, негативно сказывается на пропускной способности сети. Протокол RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 520.

Формат RIP-пакетов, которыми обмениваются динамические маршрутизаторы, выглядит следующим образом (рис. 3.20).

Рис. 3.20. Формат RIP-пакета

- Command – команда, которая определяет назначение пакета (1 – запрос; 2 – ответ). Команда-запрос производит опрос узла-маршрутизатора о его таблице маршрутизации. Команда-ответ содержит информацию о маршрутах из таблицы маршрутизации данного узла.
- Version – номер версии протокола (1 – RIPv1; 2 – RIPv2).
- Routing Domain – идентификатор RIP-системы, к которой принадлежит данное сообщение. Указывается в том случае, если не-

сколько автономных систем используют один физический канал передачи данных. Данное поле не определено в RIPv1 (равно 0).

- RIP Entry – запись маршрутной информации RIP. В RIP-пакете может содержаться от 1 до 25 таких записей.

Формат записи RIP Entry зависит от версии протокола RIP (рис. 3.21 и 22).

Биты																															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
AFI																0															
IP-address																															
0																															
0																															
Metric																															

Рис. 3.21. Формат записи RIP Entry для RIPv1

- AFI (Address Family Identifier) – тип адреса. Данное поле равно 2, что соответствует значению AF_INET (протокол IP).
- IP-address – адрес назначения в формате IPv4 (сеть или хост).
- Metric – метрика маршрута.

Биты																															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
AFI																Route Tag															
IP-address																															
Subnet Mask																															
Next hop																															
Metric																															

Рис. 3.22. Формат записи RIP Entry для RIPv2

- AFI (Address Family Identifier) – тип адреса. Данное поле равно 2, что соответствует значению AF_INET (протокол IP).
- Route Tag – тэг маршрута. Позволяет отделить «внутренние» маршруты автономной системы от «внешних» (маршруты другого IGP или EGP).
- IP-address – адрес назначения в формате IPv4 (сеть или хост).
- Subnet Mask – маска подсети.
- Next Hop – содержит IP-адрес следующего маршрутизатора при передаче пакета до места назначения. Данное поле заполняется, если протокол RIP не был включен на всех маршрутизаторах сети.
- Metric – метрика маршрута.

Рассмотрим работу протокола RIP на примере маршрутизаторов с операционной системой CIOS (оборудование Cisco). Включение данного протокола позволит маршрутизаторам, составляющим автономную систему, производить автоматический сбор сведений о логической и физической структуре данной сети, а также редактировать таблицы маршрутизации для использования оптимальных путей следования пакетов (рис. 3.23).

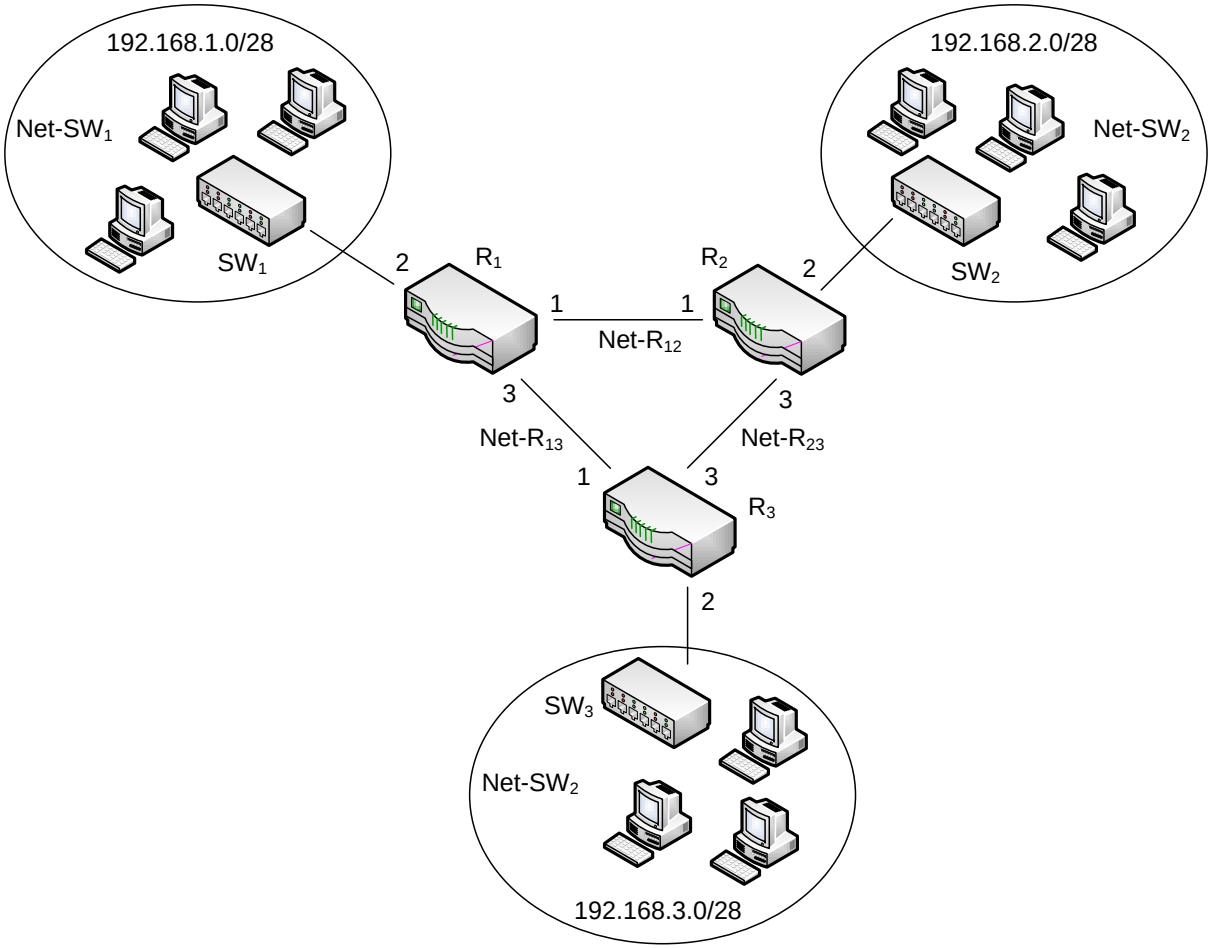


Рис. 3.23. Конфигурация сети с динамической маршрутизацией по протоколу RIPv2

Любое изменение конфигурации сети через определенный интервал времени, необходимый на обработку и рассылку обновленной информации о маршрутах, будет зафиксировано маршрутизатором, и тот внесет соответствующие изменения в свою таблицу маршрутизации. При этом остальные маршрутизаторы также будут уведомлены о произошедших изменениях.

На рис. 3.23 использованы следующие обозначения:

- Маршрутизаторы – R_1, R_2, R_3
- Коммутаторы в подсетях – SW_1, SW_2, SW_3
- Подсети верхнего контура – Net-R_{12}, Net-R_{13}, Net-R_{23}
- Подсети нижнего контура – Net-SW_1, Net-SW_2, Net-SW_3

Перед построением динамических таблиц маршрутизации, как и в случае со статическими таблицами, необходимо произвести предварительную настройку сетевых устройств – присвоить IP-адреса интерфейсам маршрутизаторов в подсетях верхнего контура (табл. 3.8), а также выделить адреса для узлов, находящихся в подсетях нижнего контура, и указать для них шлюзы по умолчанию (табл. 3.9).

Таблица 3. 8

Адресное пространство подсетей верхнего контура

Подсеть	IP-адрес	Назначение
Net-R_{12}	10.10.11.0/30	Адрес подсети
	255.255.255.252	Маска подсети
	10.10.11.1/30	R_1 , интерфейс 1
	10.10.11.2/30	R_2 , интерфейс 1
	10.10.11.3/30	Широковещательный адрес
Net-R_{13}	10.10.11.4/30	Адрес подсети
	255.255.255.252	Маска подсети
	10.10.11.5/30	R_1 , интерфейс 3
	10.10.11.6/30	R_3 , интерфейс 1
	10.10.11.7/30	Широковещательный адрес
Net-R_{23}	10.10.11.8/30	Адрес подсети
	255.255.255.252	Маска подсети
	10.10.11.9/30	R_2 , интерфейс 3
	10.10.11.10/30	R_3 , интерфейс 3
	10.10.11.11/30	Широковещательный адрес

Как видно из табл. 3.8, адресные пространства, выделенные для подсетей верхнего контура, используют маску 255.255.255.252. Такая маска позволяет всем трем подсетям связать интерфейсы маршрутизаторов без лишних затрат адресного пространства.

Таблица 3. 9

Адресное пространство подсетей нижнего контура

Подсеть	IP-адрес	Назначение
Net-SW_1	192.168.1.0/28	Адрес подсети
	255.255.255.240	Маска подсети
	192.168.1.1/28	Шлюз – R_1 , интерфейс 2
	192.168.1.2 – 192.168.1.14	Хосты
	192.168.1.15/28	Широковещательный адрес
Net-SW_2	192.168.2.0/28	Адрес подсети
	255.255.255.240	Маска подсети
	192.168.2.1/28	Шлюз – R_2 , интерфейс 2
	192.168.2.2 – 192.168.2.14	Хосты
	192.168.2.15/28	Широковещательный адрес

Net-SW$_3$	192.168.3.0/28	Адрес подсети
	255.255.255.240	Маска подсети
	192.168.3.1/28	Шлюз – R_3 , интерфейс 2
	192.168.3.2 – 192.168.3.14	Хосты
	192.168.3.15/28	Широковещательный адрес

Адресное пространство, выделенное для подсетей нижнего контура, с учетом маски 255.255.255.240 обеспечивает адресами 13 внутренних узлов в каждой подсети. Очевидно, что один IP-адрес в каждой из этих трех подсетей присваивается интерфейсу маршрутизатора, который должен быть указан для внутренних узлов шлюзом по умолчанию.

Командная оболочка CIOS позволяет осуществлять ввод команд, обеспечивающих работу протоколов RIPv1 и RIPv2. Данные команды вводятся в специальном режиме конфигурации маршрутизатора **(router)**. В частности, команда **router rip** позволяет перейти в подрежим конфигурирования протокола RIP.

Соблюдая правила ввода команд в консоли CIOS, произведем настройку интерфейсов на маршрутизаторе R_1:

```
R1> enable
R1# conf t
R1(config)# interface ethernet 0/1
R1(config -if)# no shutdown
R1(config -if)# ip address 10.10.11.1 255.255.255.252
R1(config -if)# exit
R1(config)# interface ethernet 0/3
R1(config -if)# no shutdown
R1(config -if)# ip address 10.10.11.5 255.255.255.252
R1(config -if)# exit
R1(config)# interface ethernet 0/2
R1(config -if)# no shutdown
R1(config -if)# ip address 192.168.1.1 255.255.255.240
R1(config -if)# ^Ctrl -Z
```

Аналогичным образом настроим интерфейсы на маршрутизаторе R_2:

```
R2> enable
R2# conf t
R2(config)# interface ethernet 0/1
R2(config -if)# no shutdown
R2(config -if)# ip address 10.10.11.2 255.255.255.252
R2(config -if)# exit
```

```
R2(config)# interface ethernet 0/3
R2(config -if)# no shutdown
R2(config -if)# ip address 10.10.11.9 255.255.255.252
R2(config -if)# exit
R2(config)# interface ethernet 0/2
R2(config -if)# no shutdown
R2(config -if)# ip address 192.168.2.1 255.255.255.240
R2(config -if)# ^Ctrl -Z
```

А также настроим интерфейсы на маршрутизаторе R_3:

```
R3> enable
R3# conf t
R3(config)# interface ethernet 0/1
R3(config -if)# no shutdown
R3(config -if)# ip address 10.10.11.6 255.255.255.252
R3(config -if)# exit
R3(config)# interface ethernet 0/3
R3(config -if)# no shutdown
R3(config -if)# ip address 10.10.11.10 255.255.255.252
R3(config -if)# exit
R3(config)# interface ethernet 0/2
R3(config -if)# no shutdown
R3(config -if)# ip address 192.168.3.1 255.255.255.240
R3(config -if)# ^Ctrl -Z
```

После необходимой настройки интерфейсов маршрутизаторов для работы протокола RIPv2 достаточно перечислить список подсетей, в которые входит тот или иной маршрутизатор (табл. 3.10).

Таблица 3.10

Связь маршрутизаторов с подсетями

Маршрутизатор	Обозначение подсети	IP-адрес подсети
R_1	Net-R_{12}	10.10.11.0/30
	Net-R_{13}	10.10.11.4/30
	Net-SW_1	192.168.1.0/28
R_2	Net-R_{12}	10.10.11.0/30
	Net-R_{23}	10.10.11.8/30
	Net-SW_2	192.168.2.0/28
R_3	Net-R_{13}	10.10.11.4/30
	Net-R_{23}	10.10.11.8/30
	Net-SW_3	192.168.3.0/28

Корректная настройка RIPv2 обеспечивается вводом на маршрутизаторе R_1 в управляющей консоли следующего набора команд:

```
R1> enable
R1# conf t
R1(config)# router rip
R1(config - router)# version 2
R1(config - router)# no auto-summary
R1(config - router)# network 10.10.11.0
R1(config - router)# network 10.10.11.4
R1(config - router)# network 192.168.1.0
```

Соответствующим образом настраивается протокол RIPv2 на маршрутизаторе R_2:

```
R2> enable
R2# conf t
R2(config)# router rip
R2(config - router)# version 2
R2(config - router)# no auto-summary
R2(config - router)# network 10.10.11.0
R2(config - router)# network 10.10.11.8
R2(config - router)# network 192.168.2.0
```

В управляющей консоли маршрутизатора R_3 выполняются следующие команды:

```
R3> enable
R3# conf t
R3(config)# router rip
R3(config - router)# version 2
R3(config - router)# no auto-summary
R3(config - router)# network 10.10.11.4
R3(config - router)# network 10.10.11.8
R3(config - router)# network 192.168.3.0
```

Команда **version 2** обеспечивает включение протокола RIPv2, команда **network 10.10.11.x** перечисляет сети, к которым подключены интерфейсы маршрутизаторов.

Команда **no auto-summary** отключает объединение адресов подсетей. Без этой команды произошло бы, например, объединение подсетей

10.10.11.0/30 и 10.10.11.4/30 в рамках битовой границы сети класса A, то есть в таблицу маршрутизации вместо этих двух подсетей была бы внесена запись относительно сети 10.0.0.0/8. Это привело бы к образованию ложных маршрутных записей и некорректной работе протокола RIP. Данное свойство наследовано в RIPv2 от RIPv1. Таким образом, в RIPv2 по умолчанию используется классовая адресация, ведущая к объединению подсетей.

После включения на маршрутизаторах R_1, R_2 и R_3 протокола RIPv2 и перечисления маршрутизируемых подсетей можно произвести проверку таблиц маршрутизации при помощи команды **show ip route**.

Так, например, маршрутная информация на R_1 имеет следующий вид:

```
R1# show ip route
Gateway of last resort is not set
   10.0.0.0/30 is subnetted , 3 subnets
R  10.10.11.8 [120/1] via 10.10.11.6 , 00:00:03 , Ethernet0 /3
                 [120/1] via 10.10.11.2 , 00:00:19 , Ethernet0 /1
C  10.10.11.0 is directly connected , Ethernet0 /1
C  10.10.11.4 is directly connected , Ethernet0 /3
   192.168.1.0/28 is subnetted , 1 subnets
C  192.168.1.0 is directly connected , Ethernet0 /2
   192.168.2.0/28 is subnetted , 1 subnets
R  192.168.2.0 [120/1] via 10.10.11.2 , 00:00:19 , Ethernet0 /1
   192.168.3.0/28 is subnetted , 1 subnets
R  192.168.3.0 [120/1] via 10.10.11.6 , 00:00:04 , Ethernet0 /3
```

После обмена маршрутной информацией с R_2 и R_3 маршрутизатор R_1 получает сведения о маршрутах и шлюзах ко всем удаленным сетям внутри данной автономной системы.

Запись «Gateway of last resort is not set» в заголовке маршрутной информации говорит о том, что составленная таблица маршрутизации не имеет записи маршрута по умолчанию. Символ «R» в списке маршрутов, установленный вначале строки перед адресом подсети, указывает на то, что данный маршрут был построен при помощи протокола RIP. Символ «C» означает, что подсеть напрямую подключена к указанному интерфейсу маршрутизатора.

В заключение, необходимо отметить, что относительно простые алгоритмы работы протокола RIP способны приводить к образованию, так называемых, маршрутных петель, что, в свою очередь, негативно сказывается на работе всей автономной системы. Причинами возникновения петель могут быть как сбои программного обеспечения, так и физическое разрушение каналов передачи данных.

При возникновении маршрутных петель в таблице маршрутизации IP-пакеты будут зацикливаться. Вместе с тем, необходимо учитывать правило IP-маршрутизации, при котором значение поля TTL IP-пакета, проходящего через шлюз, должно уменьшаться на одну единицу. Таким образом, перемещаясь по петле между маршрутизаторами, IP-пакеты обнуляют свое поле TTL и уничтожаются, что приводит к потере передаваемых данных.

Для предотвращения маршрутных петель в протоколе RIP используется алгоритм **split horizon** (расщепление горизонта). Принцип данного алгоритма заключается в запрете на объявление маршрута через интерфейс, с которого была получена информация о данном маршруте. Например, если маршрутизатор R_1 получил информацию от маршрутизатора R_3 о подсети 192.168.3.0/28 через интерфейс 10.10.11.5, то он не должен отправлять обратную информацию R_3, которая бы содержала данные о том, что подсеть 192.168.3.0/28 стала доступной через R_1.

В том случае, если алгоритм расщепления горизонта не активирован и происходит отказ внутреннего интерфейса R_3 (192.168.3.1), данный маршрутизатор посчитает, что существует обходной маршрут для доставки пакетов к подсети 192.168.3.0/28 через R_1. Маршрутизатор R_1 в соответствии со своей таблицей маршрутизации снова отправит эти пакеты на R3, что приведет к зацикливанию трафика.

Таким образом, исключая обратный маршрут между двумя маршрутизаторами, алгоритм расщепления горизонта, препятствует образованию маршрутных петель. Очевидно, что данный алгоритм не будет эффективен, когда автономная система состоит из трех и более маршрутизаторов.

В CIOS поддержка алгоритма расщепления горизонта включена на каждом интерфейсе маршрутизатора по умолчанию. Ее отключение производится при помощи команды управляющей консоли **no ip split-horizon**.

3.11. Протокол EIGRP

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) был разработан фирмой Cisco в конце прошлого века и поддерживается маршрутизаторами на платформе CIOS. Как и RIPv2, EIGRP поддерживает бесклассовую маршрутизацию и маски переменной длинны. Основными преимуществами данного протокола перед RIPv2 являются:

- более эффективное противостояние маршрутным петлям;
- более гибкая система вычисления метрики маршрута;
- меньшее время схождения (стабилизации) маршрутной информации;
- частичное обновление таблиц маршрутизации;
- поддерживаемая длина маршрута составляет 224 транзитных перехода вместо 16 у RIP.

В отличие от RIP данный протокол использует более широкий спектр служебных сообщений:

- **Hello** – пакеты приветствия, которые используются для обнаружения соседних узлов-маршрутизаторов, их тестирования и повторного обнаружения в случае сбоя. Для отправки пакетов применяется многоадресная рассылка (muilticast-адрес 224.0.0.10).
- **Update** – пакеты обновления маршрутов, в которых содержится информация об изменении маршрутов. Эти пакеты отправляются определенному маршрутизатору (unicast) или группе маршрутизаторов (multicast). Получение Update-пакета подтверждается отправкой специального ACK-пакета.
- **Query** – пакеты запросов, которые используются в том случае, если маршрутизатор пересчитывает какой-либо маршрут, не имея для него резервного маршрута. Он отправляет Query-запрос соседним маршрутизаторам, и, если в их таблицах маршрутизации имеется необходимый маршрут, они отвечают сообщением Reply. Если необходимого маршрута на соседних маршрутизаторах не обнаруживается, то Query-запрос пересылается соседним для них маршрутизаторам. Получение Query-запроса подтверждается ACK-пакетом.
- **Reply** – пакеты, которые маршрутизатор отправляет в ответы на Query-пакеты в случае обнаружения запрошенного маршрута в своей таблице маршрутизации. Получение Reply-пакета подтверждается отправкой ACK-пакета.
- **Acknowledgment** – unicast-пакеты, которые подтверждают получение пакетов Update, Query, Reply. ACK-пакеты содержат в себе acknowledgment number.

Гарантия получения отправленных сообщений EIGRP основана на использовании протокола Cisco – RTP, в соответствии с которым пакеты отправляются маршрутизатором на muilticast-адрес 224.0.0.10. Каждый соседний узел-маршрутизатор, получивший такой пакет, посылает подтверждение отправителю пакета о получении сообщения. При этом в каждом пакете используется два номера последовательности. Первый номер присваивается узлом-отправителем пакета и увеличивается на единицу каждый раз, когда этот узел передает новый пакет. Вместе с тем, узел-отправитель помещает в пакет номер последнего полученного пакета от получателя. Таким образом в системе сохраняется порядок пакетов.

Обмен маршрутизатора сообщениями с соседними маршрутизаторами предполагает наличие у него таблицы Neighbor Table – таблицы соседних устройств, которая является важным компонентом в работе протокола EIGRP.

Для определения соседних узлов-маршрутизаторов EIGRP использует пакеты Hello, которые рассылаются периодически с интервалом в 5 секунд. Каждый маршрутизатор формирует свою таблицу соседних

устройств, в которой перечислены подключенные к нему узлы (IP-адреса маршрутизаторов, интерфейсы данного маршрутизатора, соединенные с ними и другая полезная сетевая информация).

После заполнения таблиц соседних устройств, когда маршрутизаторы определили списки соседних маршрутизаторов, начинается обмен информацией о маршрутах – рассылка Update-пакетов. Как было отмечено выше, данные сообщения могут быть адресованы как определенному маршрутизатору, так и целой группе узлов (multicast-адрес 224.0.0.10).

Вначале маршрутизаторы обмениваются между собой всеми известными маршрутами, кроме тех, которые исключаются алгоритмом split horizon. После общего обмена маршрутами передаются только изменения в таблицах маршрутизации. Очевидно, что изменение конфигурации сети, когда меняется набор соседних узлов, приводит к новому полному обмену информацией между маршрутизаторами.

Среди особенностей протокола EIGRP необходимо отметить расчет метрики. Ее вычисление базируется на пяти составляющих:

- Bandwidth – полоса пропускания между узлом-источником и узлом-получателем пакетов;
- Delay – задержка для всего пути следования пакетов;
- Reliability – надежность на всем пути, которая оценивается на основании времени поддержания соединения;
- Loading – загрузка на всем пути следования пакетов, которая оценивается на основании частоты передаваемых пакетов и используемой полосы пропускания на интерфейсах;
- MTU – параметр, определяющий максимальный размер блока, который может быть передан на канальном уровне модели OSI.

По умолчанию для подсчета метрики применяются только Bandwidth и Delay. Использование остальных параметров, как показывает практика, приводит к частым пересчетам маршрутов.

Так как общая метрика маршрута определяется при помощи значений пропускной способности и задержки, приведем формулы для расчета данных показателей:

$$\text{Bandwidth} = (10000000 / \text{MIN}_{\text{bandwidth}}) \times 256,$$

где $\text{MIN}_{\text{bandwidth}}$ – наименьшая пропускная способность из всех интерфейсов по пути построения маршрута, которая определяется в килобитах.

$$\text{Delay} = \text{SUM}_{\text{delay}} \times 256,$$

где $\text{SUM}_{\text{delay}}$ – сумма всех задержек на всем пути построения маршрута, измеряемая в десятках микросекунд.

Определив значения пропускной способности и задержки, вычислим общую метрику маршрута:

$$\text{Metric} = \text{Bandwidth} + \text{Delay}.$$

Что касается настройки протокола EIGRP при помощи управляющей консоли CIOS, то она аналогична настройке протокола RIP.

3.12. Протокол OSPF

Рассмотренные ранее протоколы RIP и EIGRP относятся к типу дистанционно-векторных протоколов маршрутизации. Это означает, что сообщения, посылаемые соседними узлами маршрутизатора, содержат вектор расстояний или счетчик пересылок. Это позволяет маршрутизатору производить записи в свою таблицу маршрутизации на основании векторов расстояния, которые он получает от соседних узлов-маршрутизаторов.

Но существуют протоколы маршрутизации, алгоритмы которых опираются на информацию о состоянии каналов, соединяющих узлы внутри автономной сети. Так, каждый маршрутизатор производит оценку состояния связей с соседними узлами, обмениваясь с ними результатами проведенного тестирования. На основании этих данных строятся таблицы маршрутизации. Наибольшее распространение на сегодняшний день получил протокол состояния каналов OSPF.

Протокол OSPF (Open Shortest Path First) обеспечивает динамическую маршрутизацию в рамках автономной системы, содержащей большое количество узлов и имеющей сложную структуру. Так же как RIP и EIGRP, он относится к категории протоколов внутридоменной маршрутизации – IGP. Этот протокол подробно описан в документе RFC 2328.

Основными отличительными особенностями OSPF являются:

- поддержка бесклассовой маршрутизации и масок переменной длинны;
- меньшее по сравнению с RIP время стабилизации сети после изменения ее конфигурации;
- использование алгоритма Дейкстры для нахождения оптимального пути при построении маршрута;
- отсутствие ограничений на длину маршрута.

При использовании OSPF автономная система может быть поделена на отдельные области – зоны (Area) маршрутизации, в каждой из которых маршрутизация трафика между подсетями и узлами осуществляется независимо от других зон, что позволяет в значительной степени сократить необходимый объем маршрутной информации.

Также в OSPF вводится понятие опорной сети – магистрали (backbone), которая служит для связи между отдельными зонами. При этом функционирование протокола OSPF внутри автономной системы не исключает использования в выделенной зоне своего протокола маршрутизации.

Приведем пример разделения автономной системы на три зоны (рис. 3.24), где представлены:

- подсети первой зоны Area 1: Net-1, Net-2, Net-3;
- коммутаторы первой зоны SW_1, SW_2, SW_3;

- подсети второй зоны Area 2: Net-4, Net-5;
- коммутаторы второй зоны SW_4, SW_5;
- подсети третьей зоны Area 3: Net-6, Net-7, Net-8;
- коммутаторы третьей зоны: SW_6, SW_7, SW_8.

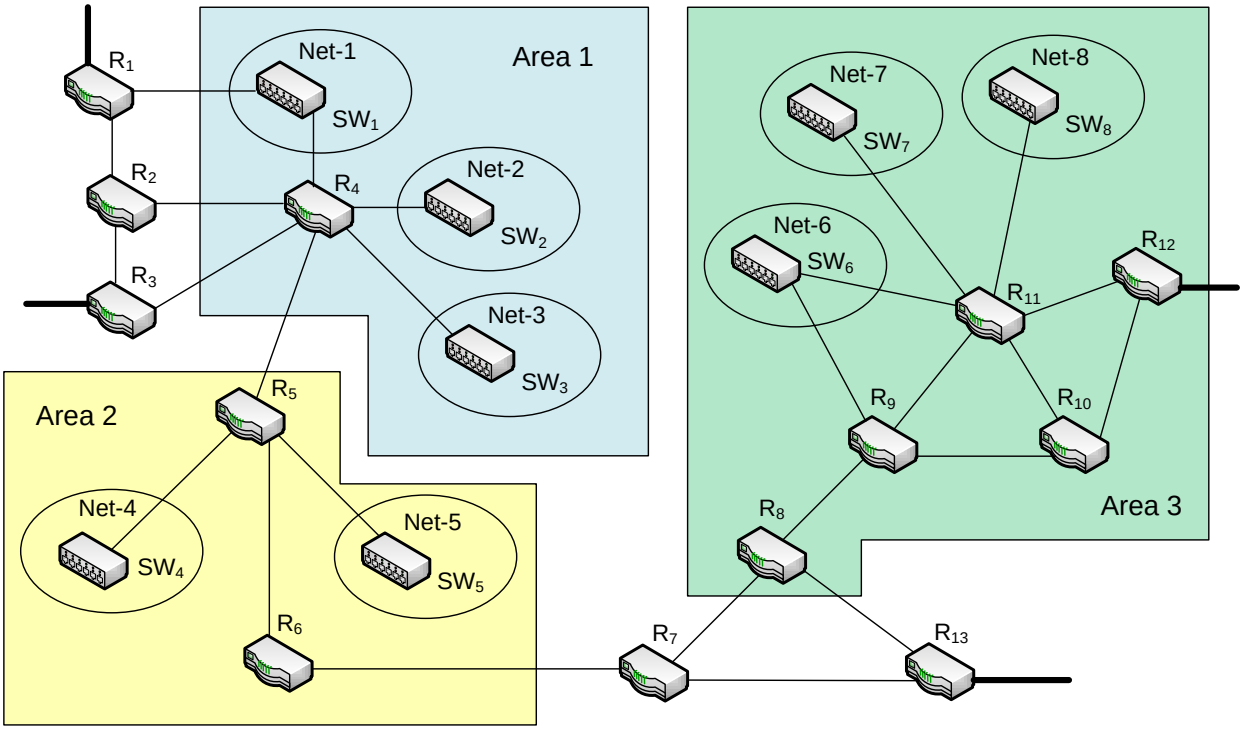


Рис. 3.24. Выделенные зоны при использовании OSPF

Маршрутизаторы на рис. 3.24 занимают определенные места в конфигурации автономной системы и, соответственно, относятся к разным категориям:

- R_9, R_{10}, R_{11} – **внутренние маршрутизаторы** (Internal Router), все интерфейсы которых принадлежат одной зоне. Такие маршрутизаторы имеют одну общую базу данных состояния каналов;
- R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8, R_{13} – **магистральные маршрутизаторы** (Backbone Router), у которых хотя бы один интерфейс относится к магистральной зоне. К ним также относятся маршрутизаторы, интерфейсы, которых не принадлежат никаким зонам кроме магистральных;
- R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8, R_{13} – **пограничные маршрутизаторы** (Area Border Router), которые соединяет одну или больше зон с магистральной зоной. У таких маршрутизаторов всегда хотя бы один интерфейс связан с магистральной зоной. При этом каждый пограничный маршрутизатор формирует отдельную базу данных состояния каналов для каждой зоны, с которой у него установлено соединение. Очевидно, что все пограничные маршрутизаторы являются

магистральными, но не каждый магистральный маршрутизатор является пограничным;

- R_1, R_3, R_{12}, R_{13} – **пограничные маршрутизаторы автономной системы** (AS boundary router), которые обменивается информацией с маршрутизаторами, находящимися в других автономных системах. Пограничный маршрутизатор автономной системы может относиться также к внутренним, пограничным или магистральным маршрутизаторам.

Необходимо отметить, что задача оптимизации маршрутов решается каждым маршрутизатором самостоятельно. И если в данный момент времени существуют два и более оптимальных маршрута, информационный трафик делится между ними поровну. Выбор оптимального маршрута производится по алгоритму Дейкстры, для которого сеть представляется в виде графа.

Покажем результат работы алгоритма Дейкстры на примере графа, вершины которого соответствуют узлам-маршрутизаторам некоторой сети, а ребра – отрезкам маршрута с заданной метрикой (рис. 3.25).

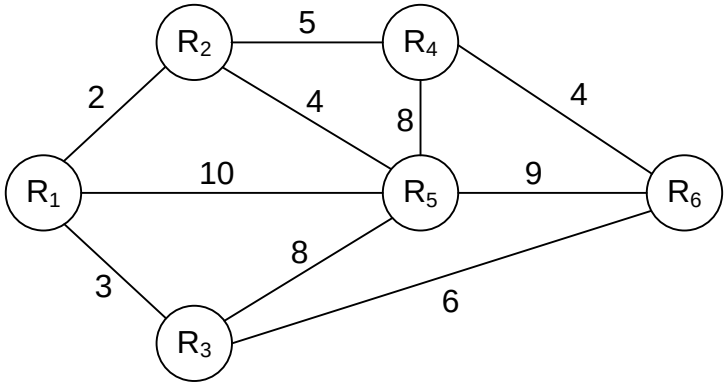


Рис. 3.25. Граф, отражающий конфигурацию сети с маршрутизаторами

Задача поиска оптимальных маршрутов состоит в нахождении путей с наименьшим суммарным значением метрики. Определим кратчайшие маршруты от узла R_1 до остальных узлов сети (табл. 3.11).

Таблица 3.11

Оптимальные маршруты от R_1 до других узлов

Маршрут	Метрика
R_1 – R_2	2
R_1 – R_3	3
R_1 – R_2 – **R_4**	7
R_1 – R_2 – **R_5**	6

R_1 – R_3 – **R_6**	9

По умолчанию при использовании протокола OSPF метрика имеет тот же физический смысл, что и в протоколе RIP, то есть длина маршрута определяется количеством пройденных транзитных участков сети. Однако, при настройке OSPF стараются задействовать более широкий спектр возможностей данного протокола.

Так в большой и сложной автономной системе метрика, как правило, характеризует оценку качества связи, опираясь на физические характеристики канала. Наибольший интерес представляют такие параметры, как пропускная способность, задержка и надежность. При этом, чем меньше значение метрики, тем лучше качество связи на этом участке сети и большая вероятность построения маршрута по данному пути.

Необходимо отметить, что кроме характеристик канала связи протокол OSPF способен учитывать также тип сервиса IP, который определен в соответствии со значением поля ToS (Type of Service) в заголовке пакета. То есть для каждого типа сервиса имеется возможность построить отдельный маршрут и организовать доставку более важных пакетов по более надежному и быстрому пути.

Еще одной отличительной особенностью OSPF является использование служебных сообщений, которые представляют собой пакеты, не затрагивающие стандартные протоколы транспортного уровня (TCP или UDP). OSPF сам назначает код (89) в протокольном поле заголовка IP пакета. При этом OSPF-сообщение инкапсулируется непосредственно в поле данных IP-пакета (рис. 3.26).

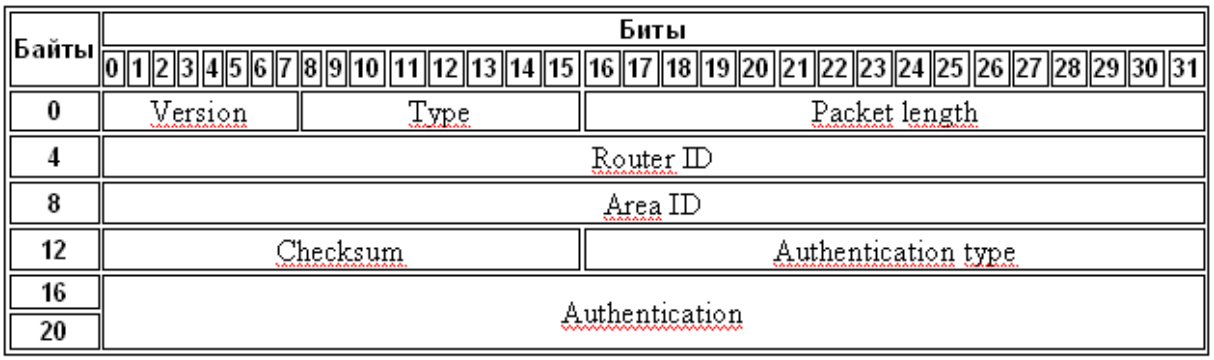


Рис. 3.26. Заголовок OSPF-сообщения

- Version – номер версии протокола OSPF. В настоящее время для сетей IPv4 используется OSPFv2.
- Type – тип OSPF-сообщения. Возможные варианты:
  1 – Hello-пакет, используется маршрутизаторами для определения соседних маршрутизаторов;

2 – сообщение Database Description, которое описывает содержание базы данных состояния канала;
3 – пакет Link State Request, который предназначен для запроса фрагмента базы данных соседнего маршрутизатора;
4 – пакет Link State Update, который предназначен для рассылки объявлений о состоянии канала;
5 – пакет Link State Acknowledgment, который подтверждает получение пакета Link State Update.

- Packet length – длина пакета вместе с заголовком.
- Router ID – уникальный идентификатор маршрутизатора (32-битное число, идентифицирующее маршрутизатор в пределах автономной системы).
- Area ID – 32-битный идентификатор зоны.
- Checksum – поле контрольной суммы.
- Authentication type – тип используемой схемы аутентификации. Возможные варианты:
  0 – аутентификация не используется;
  1 – аутентификация открытым текстом;
  2 – используется MD5-аутентификация.
- Authentication – поле данных аутентификации.

Обмен служебными сообщениями OSPF производится с целью создания маршрутизаторами баз данных состояния каналов и построения на их основе таблиц маршрутизации.

Корректная работа протокола обеспечивается за счет выполнения маршрутизаторами определенной последовательности действий и состоит из нескольких этапов.

Этап 1.

Между маршрутизаторами, на которых включен протокол OSPF, производится обмен Hello-пакетами, которые рассылаются по адресу multicast 224.0.0.5 (рис. 3.27).

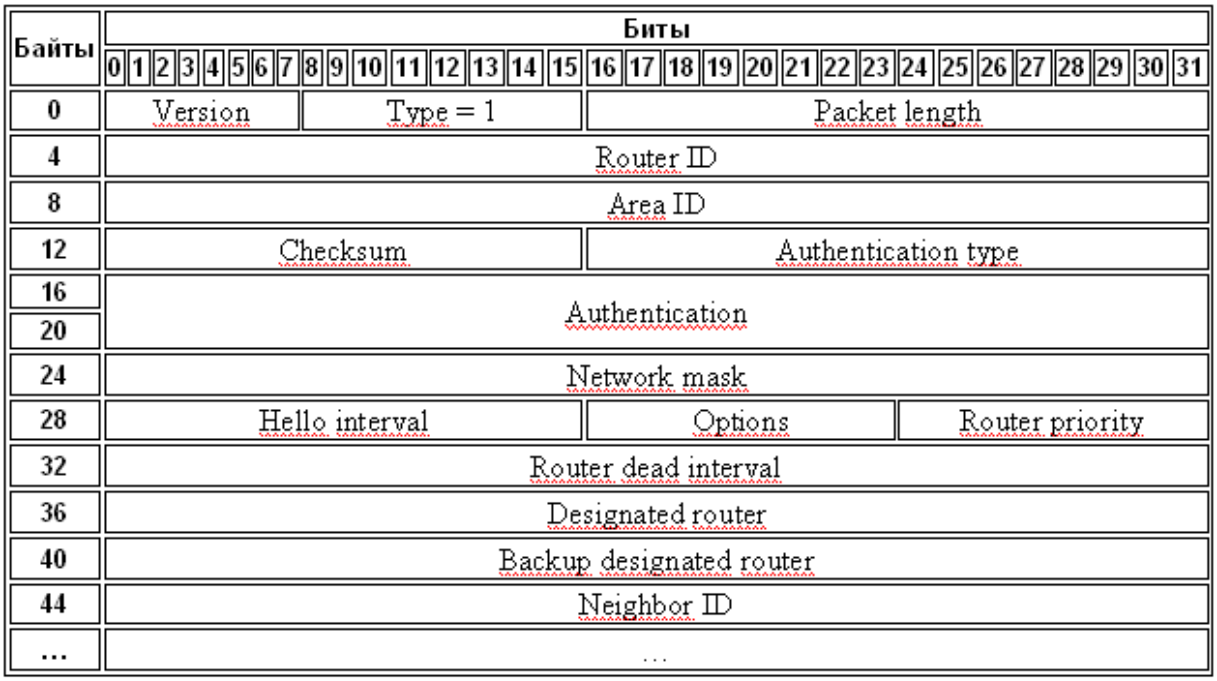


Рис. 3.27. Формат Hello-пакета OSPF

Назначение полей Hello-пакета:

- Network mask – сетевая маска интерфейса, через который отправляется Hello-пакет;
- Hello interval – интервал, который определяет частоту рассылки Hello-пакетов. В локальной сети значение данного параметра по умолчанию составляет 10 секунд;
- Options – поле опций, которое описывает возможности маршрутизатора;
- Router priority – приоритет маршрутизатора. Этот параметр влияет на выбор данного узла в качестве маршрутизатора Designated Router, который в дальнейшем будет контролировать рассылку объявлений о состоянии каналов между остальными маршрутизаторами;
- Router dead interval – интервал времени, в течение которого маршрутизатор ожидает ответа от соседних узлов;
- Designated router – IP-адрес узла, назначенного в качестве маршрутизатора Designated Router (используется в сетях с множественным доступом);
- Backup designated router – IP-адрес узла, назначенного в качестве Backup Designated Router (резервного для Designated Router);
- Neighbor ID – идентификатор соседнего узла. Составляется список идентификаторов соседних с маршрутизатором узлов, от которых им были получены Hello-пакеты в течение времени, заданного в поле Router dead interval.

Маршрутизаторы, связанные между собой общим каналом передачи данных, становятся соседними узлами по отношению друг к другу в том случае, если им удается успешно обменяться Hello-пакетами.

Этап 2.

На данном этапе маршрутизаторы стремятся перейти в состояние смежности. Целью данной операции является синхронизация между маршрутизаторами баз данных состояния каналов, для чего происходит обмен специальными пакетами типа Database Description, которые содержат только описание баз данных состояния каналов маршрутизаторов (рис. 3.28).

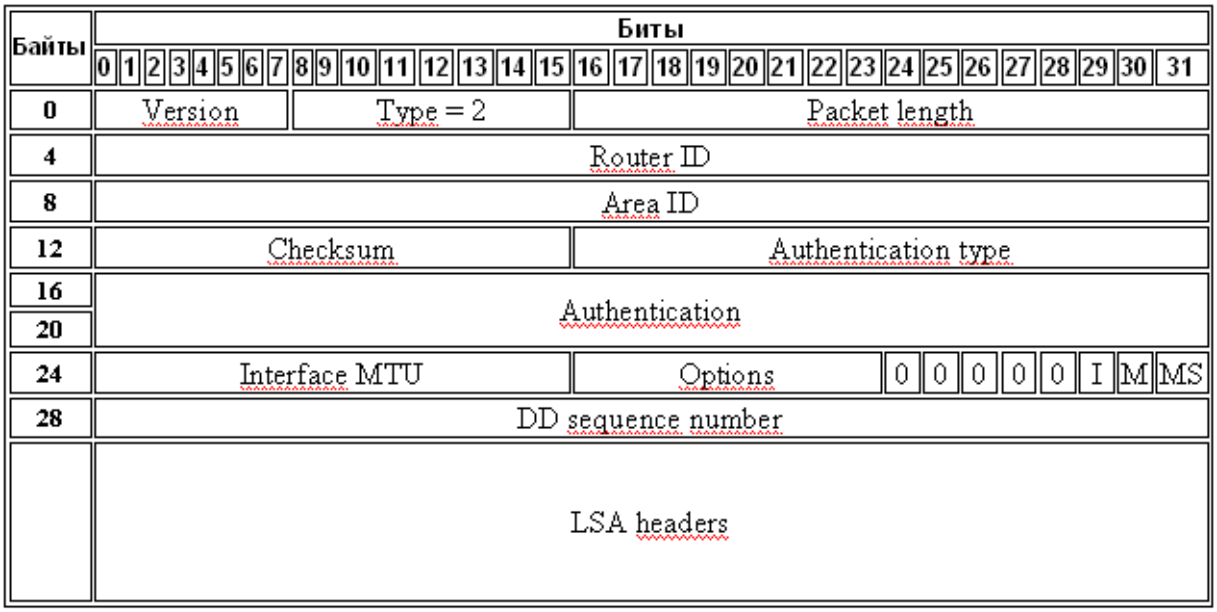


Рис. 3.28. Формат пакета Database Description

Назначение полей пакета Database Description:

- Interface MTU – размер в байтах максимального IP-пакета, который может быть отправлен через данный интерфейс без фрагментации;
- I-бит – устанавливается для первого пакета в последовательности;
- M-бит – указывает наличие последующих дополнительных пакетов;
- MS-бит – устанавливается для ведущего, сбрасывается для ведомого;
- DD sequence number – в начальном пакете устанавливается на уникальное значение, при передаче каждого последующего пакета увеличивается на единицу, пока не будет передана вся база данных;
- LSA headers – массив заголовков объявлений состояния каналов, хранящийся в базе данных маршрутизатора.

Объявление LSA (Link State Advertisement) фактически описывает состояние канала между двумя маршрутизаторами. Множество всех LSA образует базу данных состояния каналов LSDB (Link State Database), которая содержит список всех записей о состоянии каналов.

Объявления LSA (Link State Advertisement) бывают нескольких типов:

- **Router LSA** – объявление о состоянии каналов маршрутизатора. Такие LSA распространяются каждым маршрутизатором в пределах своей зоны. В них содержится описание всех каналов маршрутизатора и их метрика;
- **Network LSA** – объявление о состоянии каналов сети, которые распространяется маршрутизатором типа Designated Router в сетях с множественным доступом в пределах одной зоны;
- **Network Summary LSA** – суммарное объявление о состоянии каналов сети. Такие объявления распространяют пограничные маршрутизаторы. В них учитываются только маршруты, направленные к сетям, расположенным вне зоны и не описываются маршруты внутри автономной системы;
- **ASBR Summary LSA** – суммарное объявление о состоянии каналов, рассылаемое пограничными маршрутизаторами;
- **AS External LSA** – объявления, рассылаемые пограничными маршрутизаторами и характеризующие состоянии внешних каналов автономной системы;
- **AS External LSA for NSSA** – объявления о состоянии внешних каналов автономной системы в NSSA зоне (зона, изолированная от остальных зон автономной системы, но работающая с внешними маршрутами).

Обмен массивами заголовков LSA между маршрутизаторами позволяет избежать пересылки всей базы данных. Как правило, требуется пополнить базы данных маршрутизаторов отдельными недостающими записями.

Таким образом, каждый маршрутизатор формирует список записей базы данных, которые он должен запросить, и отправляет пакеты запросов о состоянии связей Link State Request нужному маршрутизатору (рис. 3.29).

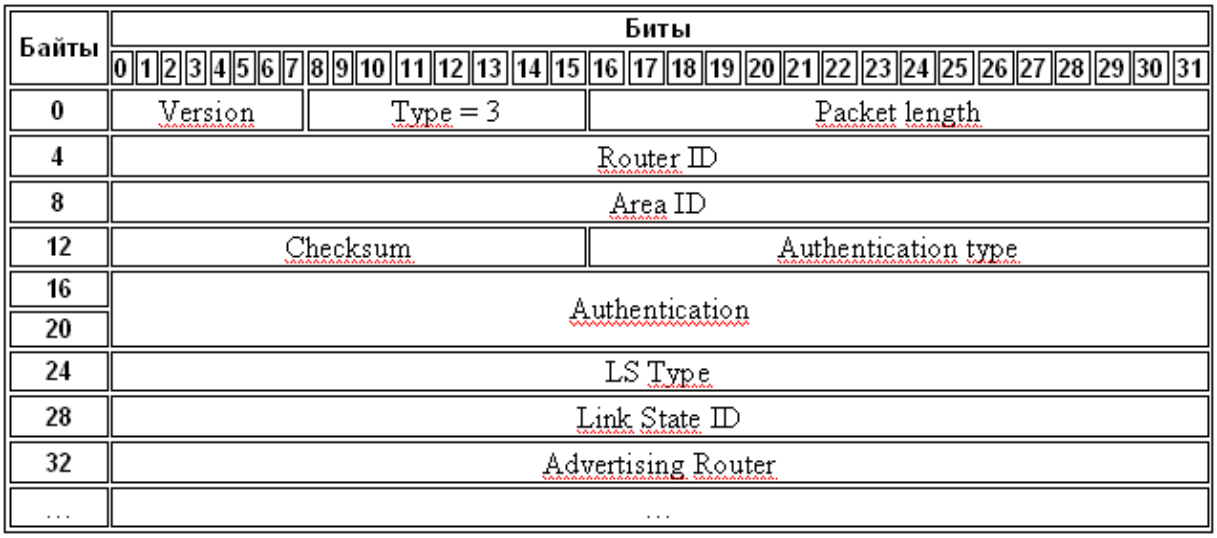


Рис. 3.29. Формат пакета Link State Request

Назначение полей пакета Link State Request:

- LS Type – тип объявления о состоянии канала;
- Link State ID – идентификатор домена маршрутизации;
- Advertising Router – идентификатор маршрутизатора, создавшего объявление о состоянии канала.

В ответ от маршрутизатора, получившего пакет Link State Request, приходит нужная запись LSA в пакетах объявления о состоянии канала Link State Update (рис. 3.30).

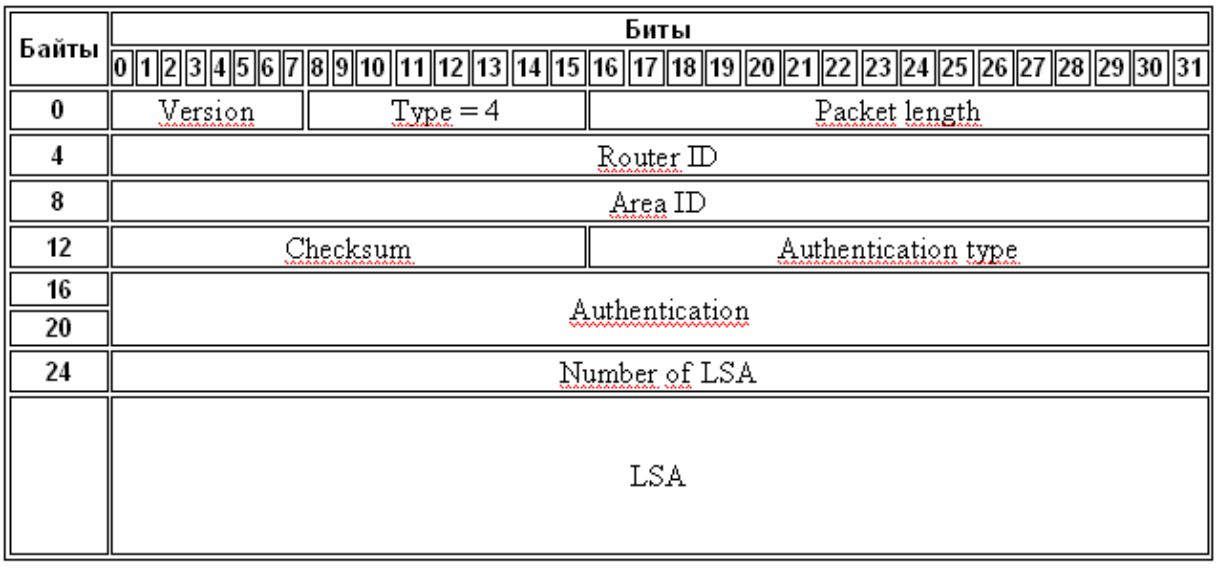


Рис. 3.30. Формат пакета Link State Update

В поле Number of LSA (рис. 3.30) записывается количество объявлений о состоянии канала, содержащихся в данном пакете.

Таким образом происходит синхронизация базы данных состояния каналов связи LSDB внутри каждой зоны.

Этап 3.

После синхронизации LSDB каждый маршрутизатор, используя алгоритм Дейкстры, вычисляет кратчайший путь без петель до конечных пунктов следования пакетов. Вместе этим происходит заполнение таблиц маршрутизации на маршрутизаторах.

Однако, любые изменения в конфигурации сети (добавление новых связей или исчезновения старых), требуют от маршрутизаторов, которых непосредственно коснулась данная ситуация, изменить свою копию базы данных и в соответствии с протоколом OSPF оповестить остальные маршрутизаторы о произошедших изменениях.

Каждый маршрутизатор, вносящий изменения в свою базу данных состояния каналов, посылает соответствующий пакет Link State Update маршрутизаторам, с которыми он находится в состоянии смежности.

Маршрутизаторы, принявшие пакет от смежного маршрутизатора, подтверждают его получение ответным пакетом Link State Acknowledgment (рис. 3.31).

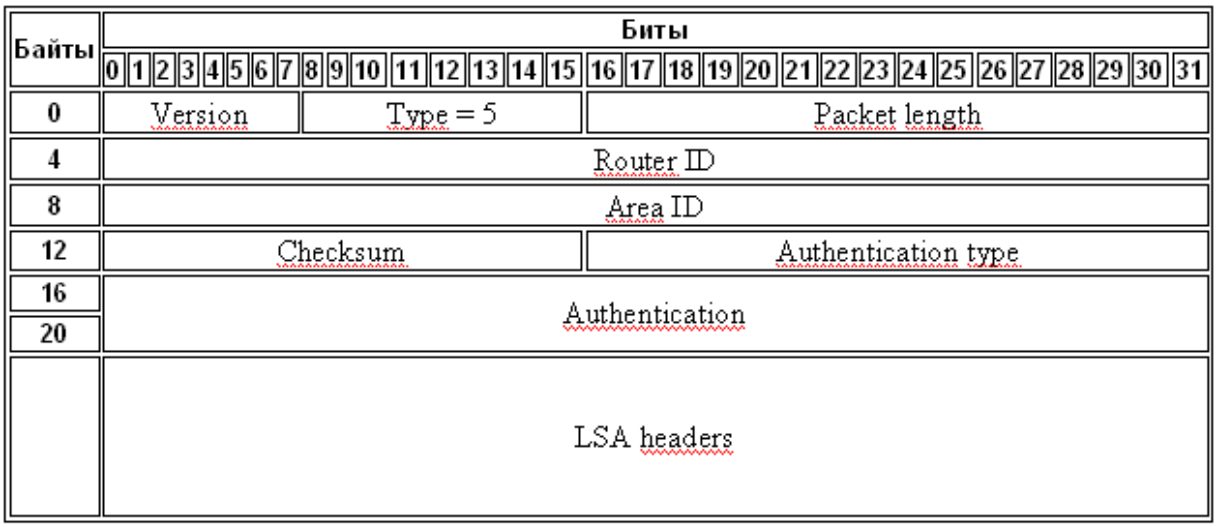


Рис. 3.31. Формат пакета Link State Acknowledgment

После этого они записывают переданную в Link State Update информацию в свою базу данных состояния каналов и рассылают копию объявления другим смежным с ними маршрутизаторам.

Рассылая объявления внутри одной зоны, все маршрутизаторы продолжают строить идентичную базу данных LSDB, на основании которой производится обновление таблиц маршрутизации.

3.13. Протокол BGP

BGP (Border Gateway Protocol) – протокол граничного шлюза, который является основным протоколом динамической маршрутизации в Интернете. Данный протокол относится к категории протоколов междоменной маршрутизации EGP и предназначен для организации взаимодействия между маршрутизаторами, расположенными в разных автономных системах.

Корректная работа BGP обеспечивается наличием в автономных системах BGP-маршрутизаторов, которые обмениваются маршрутной информацией, становясь BGP-соседями. Связь между ними устанавливается по протоколу TCP (порт 179). При этом соседи, принадлежащие разным автономным системам, должны быть напрямую доступны друг другу.

В дальнейшем BGP-соседи рассылают друг другу векторы путей. В отличие от вектора расстояний, который использовался в RIP, вектор путей помимо адреса сети и расстояния до нее содержит целый список атрибутов, характеризующих маршрут от данного маршрутизатора до указанной сети.

Служебная информация в протоколе BGP передается при помощи BGP-сообщений, заголовок которых имеет вид (рис. 3.32).

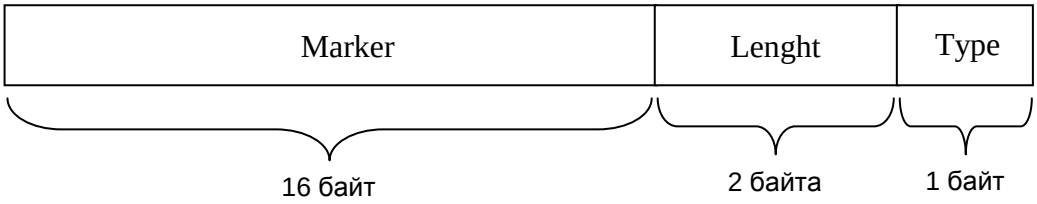


Рис. 3.32. Формат заголовка BGP-сообщения

- **Marker** – поле, которое используется в заголовке для совместимости, заполнено единицами;
- **Length** – общая длина сообщения в байтах, включая заголовок (от 19 до 4096);
- **Type** – тип передаваемого сообщения: 1 – Open; 2 – Update; 3 – Notification; 4 – Keepalive.

Сообщения в BGP бывают четырех типов.

Open – отправляется после установки TCP-соединения с соседним BGP-маршрутизатором для предложения ему стать BGP-соседом.

Keepalive – сообщение в ответ на сообщение **Open** от соседнего BGP-маршрутизатора, дающего согласие стать BGP-соседом. Используется также для поддержания открытого соединения между BGP-соседями, для этого BGP-соседи обмениваются данными сообщениями через определенные интервалы времени.

Notification – сообщение от соседнего BGP-маршрутизатора, предназначенное для информирования BGP-соседа о причине закрытия соединения.

Update – сообщение, которое предназначено для обновления маршрутной информации. Так, после установки соединения с помощью этого сообщения маршрутизатор сообщает своему BGP-соседу обо всех необходимых маршрутах. В дальнейшем происходит передача информации только о добавленных или удаленных маршрутах.

Подробное описание BGP приведено в документах RFC 4271 и RFC 4274.

3.14. Multicast

Существующие на сегодняшний день формы обмена сетевым трафиком позволяют полностью решить задачи, которые возникают при организации той или иной системы передачи данных.

Простейшей формой обмена данными является **unicast**, основной принцип которого заключается в организации соединения между двумя определенными узлами сети. Сформированный при этом сокет четко определяет IP-адреса и порты сервера и клиента, а также протокол транспортного уровня, обеспечивающий порядок доставки пакетов от источника к получателю.

По такому принципу построено большинство клиент-серверных приложений, когда программа-сервер, запущенная на отдельном хосте, ожидает подключения клиентов, прослушивая определенный порт. Клиентское приложение соединяется с сервером, отправляя в прослушиваемый порт необходимые данные. Обмен пакетами по прослушиваемому сервером порту позволит организовать связь лишь с одним клиентом. Поэтому разработчики клиент-серверных приложений стремятся создать для каждого нового обратившегося к серверу клиента отдельный сокет, используя порты из так называемого расширенного набора, которые не зарезервированы сервисами операционной системы. Таким образом, каждое подключенное клиентское приложение организовывает новое соединение и обменивается данными с серверным приложением независимо друг от друга (рис. 3.33).

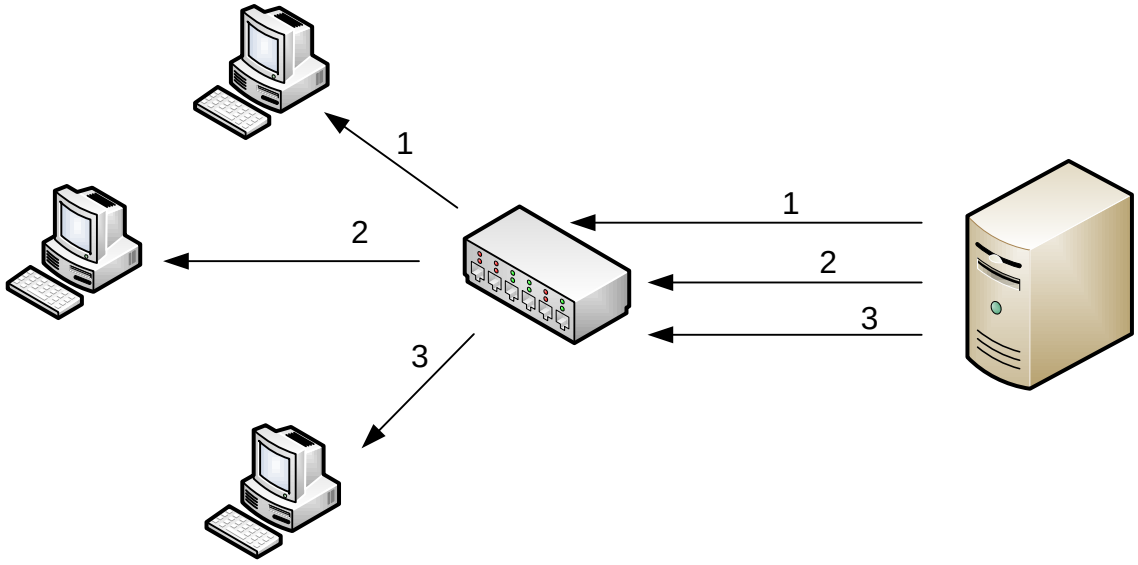


Рис. 3.33. Принцип организации unicast-вещания сервера с тремя клиентами

Из рис. 3.33 видно, что каждый клиент получает свою порцию трафика. В том случае, если клиенты получают от сервера разную по содержанию информацию, то такой метод вещания является оптимальным и не требует каких-либо доработок.

Теперь представим, что информация, передаваемая сервером в сеть для каждого клиента идентична, например, все три хоста одновременно запрашивают видеопоток с одной и той же камеры. В этом случае сервер должен открыть с клиентами три сокета и передать три раза одни и те же по содержанию пакеты. Очевидно, что в случае использования канала с большой пропускной способностью влияние «лишнего» трафика в данном примере будет незначительным. Но при этом необходимо учесть, что увеличение источников такого трафика в дальнейшем неизбежно приведет к снижению эффективности использования пропускной способности каналов.

Для решения этой проблемы была разработана технология групповой адресации, которая представляет собой расширение IP-адресации, позволяющее направить одну копию пакета от узла-отправителя всем получателям, зарегистрированным в определенной группе. Таким образом, использование принципов групповой адресации позволяет организовать **multicast** – специальную форму широковещания (рис. 3.34).

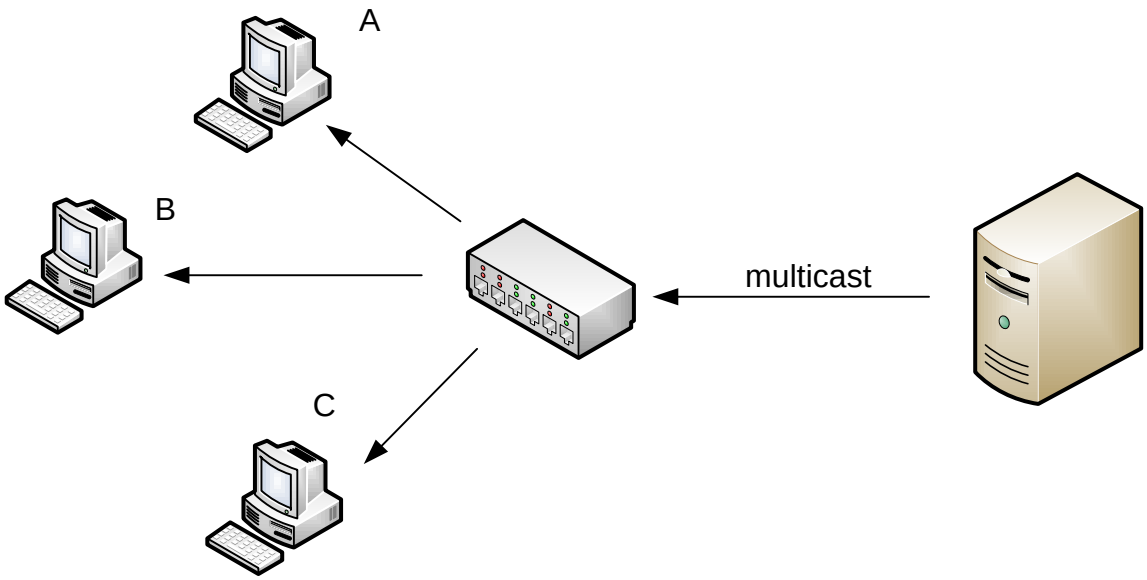


Рис. 3.34. Принцип организации multicast-вещания сервера с тремя клиентами

На рис. 3.34 показано, что хосты A, B и C, запросившие одинаковую информацию с сервера, получают каждый свою копию данных. Но трафик между сервером и коммутатором не умножается на количество клиентов, как это было в случае с unicast. В этом случае имеется некоторое сходство multicast с broadcast. Но в отличие от broadcast-вещания, при котором все хосты (рис. 3.34) всегда будут получать трафик от сервера, протоколы, поддерживающие multicast, обеспечат выборочную доставку пакетов отдельным хостам, запросившим данную информацию.

Для организации группового вещания в локальной сети необходимо соблюдение правил на всем пути следования multicast-трафика от источника до получателя.

Во-первых, организация multicast-источника подразумевает некоторое аппаратно-программное средство, которое отправляет в сеть трафик, указывая в поле получателей пакетов адрес сети класса D. Это диапазон адресов с 224.0.0.0 до 239.255.255.255. Исключив из него адреса, зарезервированные для протоколов маршрутизации (224.0.0.0 – 224.0.0.255) получим огромный диапазон multicast-адресов, которые могут быть использованы для организации multicast-групп.

Во-вторых, включение вещания в группу многоадресной рассылки требует последующего контроля за распространением multicast-пакетов, так как неорганизованное распространение данного вида трафика фактически превращается в широковещательную рассылку broadcast. Это негативно сказывается на общей загрузке сети.

Контроль над multicast-трафиком обеспечивается коммутатором L3 при помощи протокола IGMP (Internet Group Management Protocol), кото-

рый, препятствуя бесконтрольному распространению трафика, организовывает группы многоадресного вещания. Протокол IGMP подробно описан в документе RFC 3376.

В-третьих, все коммутаторы, расположенные на пути следования multicast-трафика за коммутатором, на котором был включен IGMP, требуют активации функции IGMP-snooping. Это необходимо коммутаторам для отслеживания служебных сообщений IGMP между получателем и коммутатором, контролирующим группы многоадресной рассылки. Фактически IGMP-snooping строит на промежуточном коммутаторе таблицы, записывая в них multicast-группы, трафик от которых проходит через данный коммутатор до получателей.

После включения функции IGMP-snooping коммутатор начинает анализировать все IGMP-сообщения между подключенными к нему узлами. Обнаружив IGMP-запрос отдельного узла на подключение к multicast-группе, коммутатор делает запись в свою таблицу multicast-групп, связывая группу многоадресной рассылки с физическим портом, к которому подключен данный узел-получатель multicast-трафика. Аналогично, при отключении узла-получателя от multict-группы коммутатор удаляет соответствующую запись.

Таким образом, функция L2 IGMP-snooping выполняет важную задачу – предотвращает широковещательную ретрансляцию multicast-трафика на те узлы, которые не отправляли запросов на подключение в multicast-группу и не являются его потребителями. Такой подход позволяет коммутаторам ограничить распространение multicast-трафика на своих портах, существенно снизив общую нагрузку на локальную сеть (рис. 3.35).

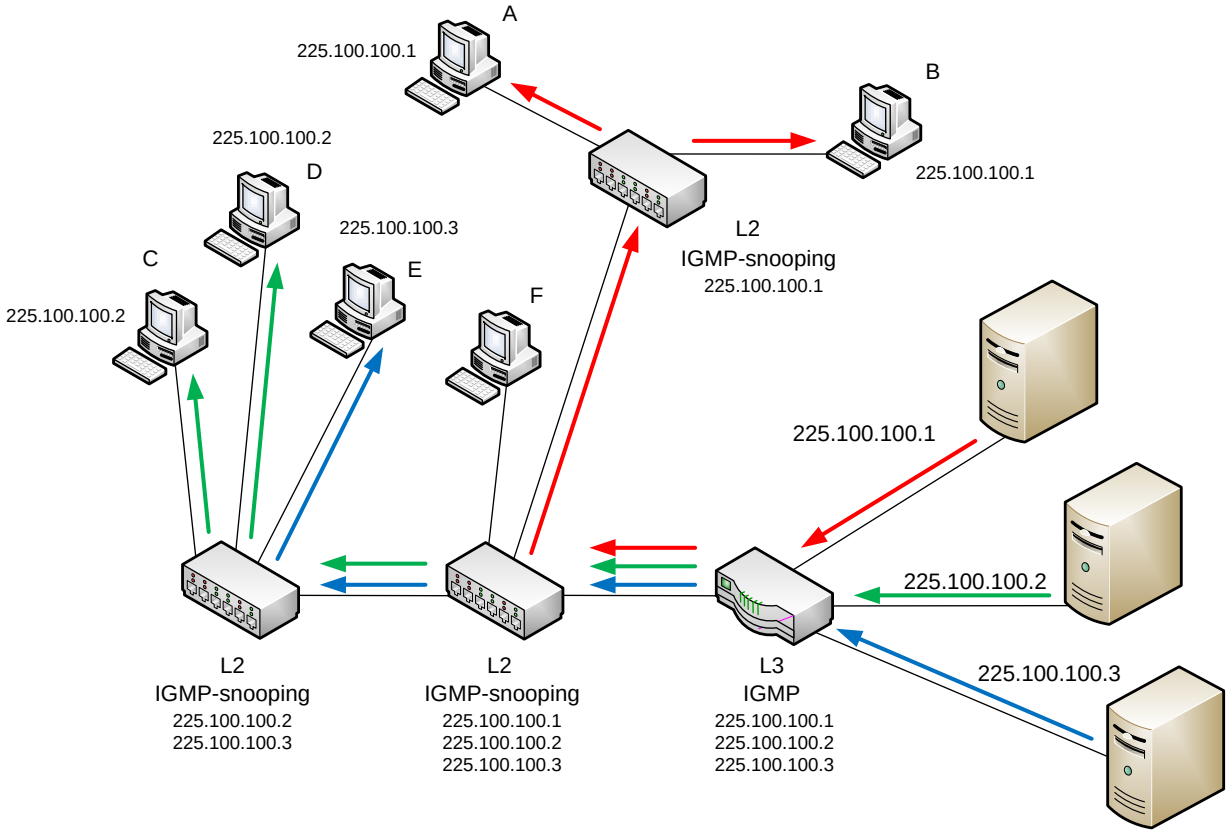


Рис. 3.35. Организация multicast-вещания в локальной сети

На рис. 3.35 показано распределение multicast-трафика в локальной сети, где используется один коммутатор L3 с включенным протоколом IGMP и три коммутатора L2 с функцией IGMP-snooping. Источниками multicast в данном случае являются серверы, которые вещают в сеть multicast-потоки: 225.100.100.1, 225.100.100.2, 255.100.100.3. Получателями multicast-трафика являются хосты, соединенные с коммутаторами L2:

- хосты A и B являются членами группы 225.100.100.1;
- хосты C и D являются членами группы 225.100.100.2;
- хост E является членом группы 225.100.100.3;
- хост F не входит ни в одну группу.

Для того, чтобы стать членом multicast-группы, узел-получатель должен использовать соответствующие программные модули, позволяющие ему организовать запрос на маршрутизатор с протоколом IGMP. Аналогичным образом потребитель multicast-трафика отправляет сообщение о том, что собирается покинуть группу.

Группа многоадресного вещания создается на коммутаторе с протоколом IGMP при первом запросе заинтересованного в ней узла. Все последующие узлы-получатели, отправляющие запросы на подключения к ней, становятся членами уже созданной группы.

Маршрутизатор, в свою очередь, производит периодический опрос членов групп, ожидая подтверждения того, что они продолжают оставаться потребителями multicast-трафика. Если такое подтверждение приходит, то отправивший его узел-получатель продолжает оставаться членом multicast-группы и получать трафик. Если же в течение заданного протоколом промежутка времени никто из членов группы не подтвердит заинтересованность в ней, группа будет удалена.

3.15. Маршрутизация multicast

Организация многоадресного вещания в локальной сети, состоящей из нескольких подсетей, порождает задачу маршрутизации multicast-трафика от источника до получателя. Для ее решения был разработан специальный протокол PIM (Protocol Independent Multicast), варианты которого – PIM-SM (Spare Mode) и PIM-DM (Dense Mode) – подробно описаны в документах RFC 4601 и RFC 3973.

Рассмотрим пример организации многоадресного вещания в локальной сети, состоящей из трех подсетей (рис. 3.36).

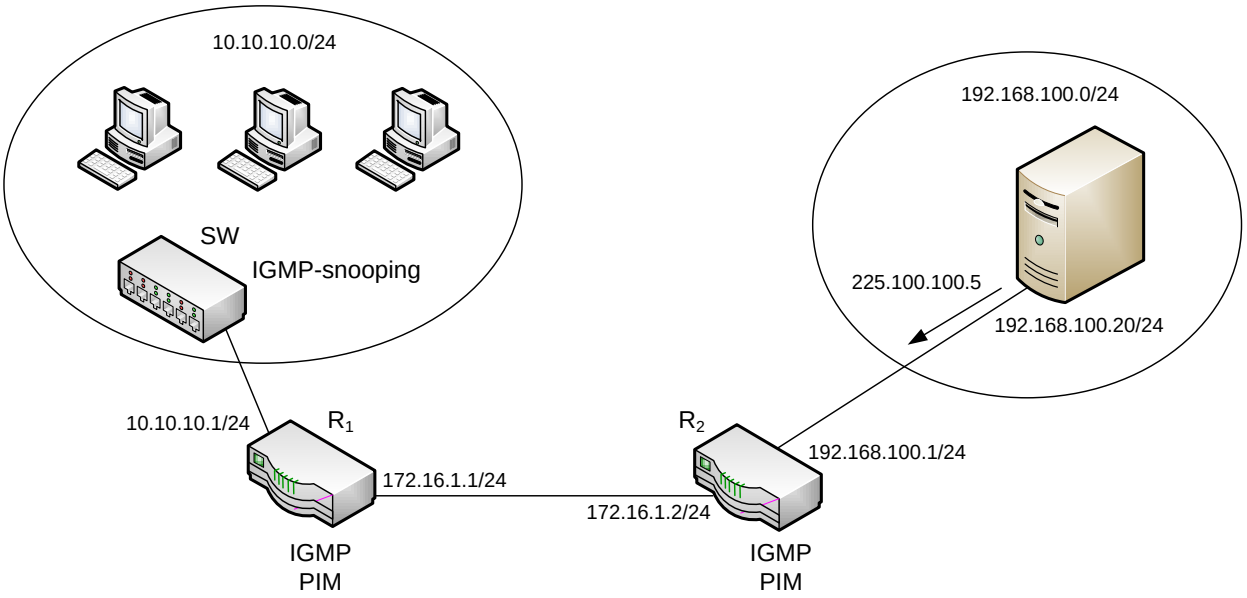


Рис. 3.36. Маршрутизация multicast-трафика в локальной сети

Первая подсеть – 192.168.100.0/24 выделена для сервера-источника multicast-трафика (192.168.100.20/24), который вещает в группу 225.100.100.5. Также в этой подсети находится один из интерфейсов маршрутизатора R_2 (192.168.100.1), который является для сервера-источника шлюзом по умолчанию.

Вторая подсеть – 172.16.1.0/24 включает интерфейсы маршрутизаторов R_1 (172.16.1.1/24) и R_2 (172.16.1.2/24), на которых активированы протоколы IGMP и PIM (PIM-SM или PIM-DM).

Третья подсеть – 10.10.10.0/24 используется хостами, которые отправляют IGMP-запросы на маршрутизатор R_2 для подписки на групповую рассылку multicast-трафика с адреса 225.100.100.5. Шлюзом для этих хостов является интерфейс маршрутизатор R_1, интерфейс которого (10.10.10.1/24) также подключен к данной сети. При этом коммутатор SW, находящийся в сети, использует функцию IGMP-snooping для корректного распространения multicast-трафика в сети 10.10.10.0/24.

Сравнивая протоколы PIM-SM и PIM-DM, имеет смысл упомянуть о структуре заголовка пакетов PIM, инкапсулируемых в IP-пакеты с номером протокола 103, и перечислить типы сообщений, которые используются данными протоколами (рис. 3.37).

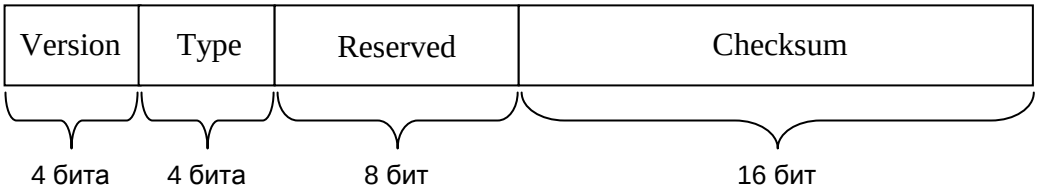


Рис. 3.37. Структура заголовка пакета PIMv2

- Version – версия протокола – 2 (наиболее распространенная).
- Reserved – в сообщениях PIMv2 данное поле заполнено нулями.
- Type – тип сообщения:
  - 0 – Hello
  - 1 – Register (используется только в PIM-SM)
  - 2 – Register Stop (используется только в PIM-SM)
  - 3 – Join/Prune
  - 4 – Bootstrap (используется только в PIM-SM)
  - 5 – Assert
  - 6 – Graft (используется только в PIM-DM)
  - 7 – Graft-Ack (используется только в PIM-DM)
  - 8 – Candidate-RP-Advertisement (используется только в PIM-SM)
- Checksum – контрольная сумма.

Как показано выше, протоколы PIM-DM и PIM-SM значительно отличаются набором используемых сообщений, что говорит о разнородности применяемых ими алгоритмов.

Структура сообщений PIM и их назначение, а также алгоритмы работы протоколов PIM-DM и PIM-SM, как уже было сказано, подробно описаны в документах RFC 4601 и RFC 3973. Отметим лишь, что протокол PIM-

DM в отличие от PIM-SM нацелен, как правило, на сети с высокой плотностью получателей multicast-трафика в отдельных подсетях. PIM-SM, в свою очередь, целесообразно использовать в том случае, если подписчики на группы многоадресной рассылки произвольно распределены по всей сети и связаны с источниками multicast-трафика каналами, ограниченными по пропускной способности.

3.16. Трансляция адресов

Интеграция частных локальных сетей, при построении которых используются рекомендуемые диапазоны IP-адресов (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), в глобальные сети требует выполнения специальной процедуры преобразования этих адресов в публичные адреса, задействованные в таблицах глобальной маршрутизации Интернет. Данный функционал обеспечивается маршрутизаторами при помощи механизма NAT (Network Address Translation) – трансляции сетевых адресов, который подробно описан в документах RFC 1631 и RFC 3022.

NAT производит замену в поле обратного адреса источника (Source IP) при прохождении пакета в одну сторону. Такая схема часто используется для доступа в Интернет пользователями локальной сети с внутренними адресами. Рассмотрим пример использования NAT (рис. 3.38).

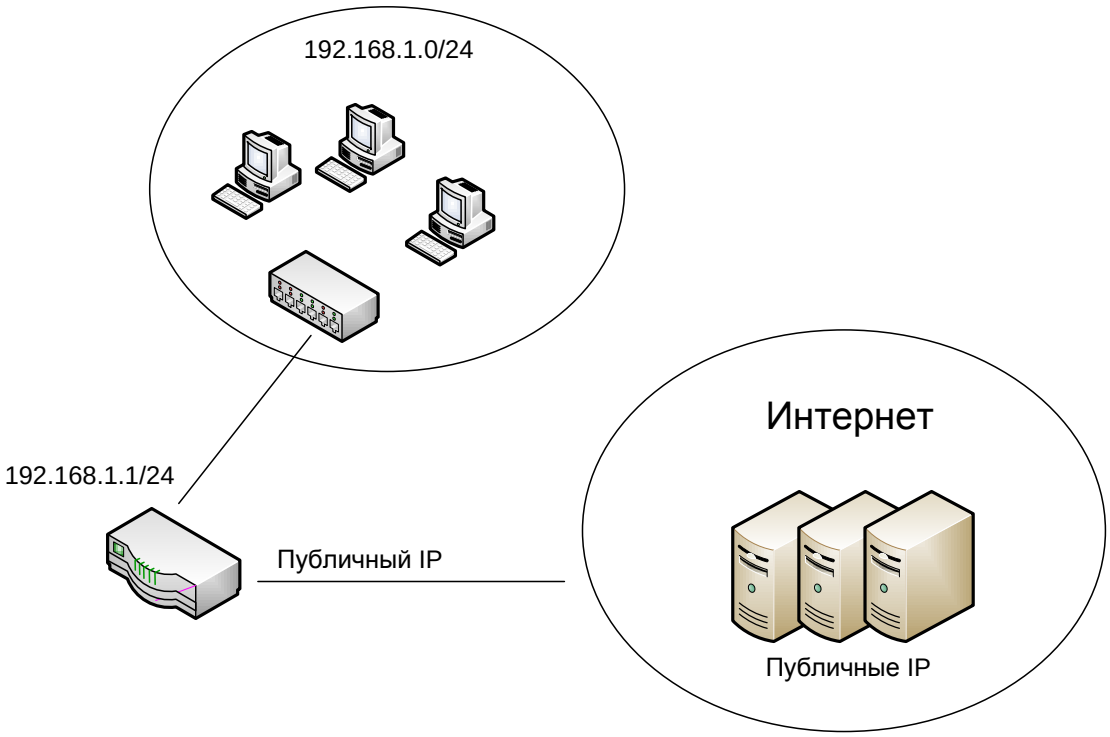


Рис. 3.38. Организация NAT через маршрутизатор

Пускай на узле внутренней сети (например, хост 192.168.1.2) запущено клиентское приложение, которое должно установить связь с серверным приложением на узле, расположенном за пределами локальной сети в Интернете. Для этого узел 192.168.1.2 открывает сокет, определяемый IP-адресами клиента и сервера, портами клиента и сервера, а также протоколом транспортного уровня.

При отправке данных в сокет IP-адрес и порт клиента (узел-отправитель с клиентским приложением) записываются в IP-пакет в поля параметров источника. Поля параметров получателя содержат IP-адрес и порт сервера. Учитывая, что узел-получатель пакета расположен за пределами локальной сети, хост 192.168.1.2 отправляет данный пакет на свой шлюз по умолчанию (192.168.1.1), где включен NAT.

Механизм NAT предусматривает хранение в маршрутизаторе таблицы, где устанавливается соответствие между внутренними IP-адресом и портом клиента и внешними IP-адресом и портом, которые будут использоваться в текущем сеансе связи с сервером вместо внутренних. Получив исходящий пакет от клиента, маршрутизатор производит соответствующую запись в таблицу NAT, регистрируя устанавливаемый сеанс связи. После этого, заменив в пакете поля источника (внутренние IP-адрес и порт клиента на внешние IP-адрес и порт NAT), маршрутизатор отправляет пакет на сервер в Интернете.

Получив пакет, сервер считает, что узлом-отправителем является маршрутизатор, IP-адрес которого указан в соответствующем поле заголовка пакета. Таким образом, все ответные пакеты сервера будут адресованы маршрутизатору.

Принимая ответные пакеты сервера, маршрутизатор анализирует их содержимое на основе своей таблицы NAT. Если в таблице будет найдена запись о сеансе, к которому относятся данные пакеты, произойдет обратное преобразование. Маршрутизатор произведет замену внешних IP-адреса и порта в полях назначения пакетов на внутренние IP-адрес и порт клиента.

Как показано выше, использование механизма NAT позволяет клиенту, находящемуся в частной сети и не имеющему индивидуального публичного адреса, обмениваться данными с внешними хостами в Интернете. Очевидным преимуществом данной схемы подключения является экономия публичных IP-адресов, так как все хосты, выходящие в Интернет через NAT, используют один внешний IP-адрес, выделенный провайдером.

При этом все серверы, к которым поступают пакеты от хостов локальной сети, обмениваются информацией только с их маршрутизатором и не могут выступать инициаторами обмена данными с этими хостами. Таким образом, использование механизма трансляции адресов позволяет ограничить снаружи доступ к внутренним узлам локальной сети, обеспечивая самим узлам доступ к внешним ресурсам.

В качестве маршрутизатора с функцией NAT может выступать как коммутатор третьего уровня L3, так и компьютер, оснащенный двумя сетевыми картами. Один сетевой интерфейс LAN (Local Area Network) подключен к частной локальной сети, другой – WAN (World Area Network) – обращен в сторону внешней сети. При этом должна обеспечиваться поддержка NAT средствами операционной системы, как, например, это реализовано в ОС Windows.

Когда в компьютере под управлением ОС Windows установлено более одной сетевой карты, в свойствах каждого сетевого интерфейса на закладке «Дополнительно» присутствует элемент управления общим доступом к Интернету. Для включения NAT необходимо определить сетевую карту, которая будет обращена к внешней сети, и установить для нее соответствующий флаг разрешения (рис. 3.39).

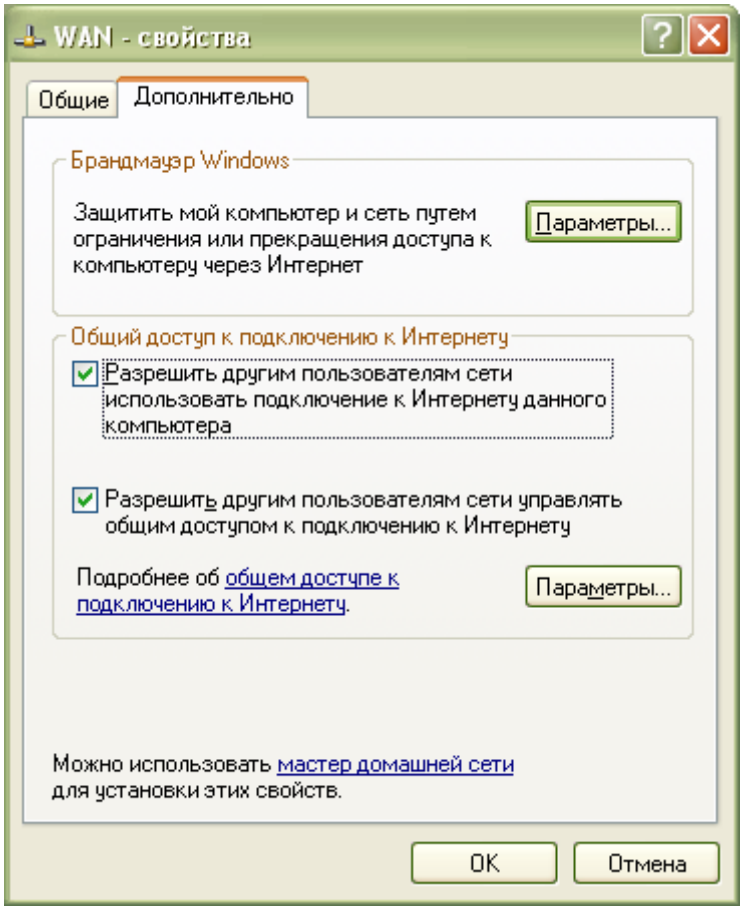


Рис. 3.39. Включение NAT в ОС Windows

IP-адрес второго сетевого интерфейса, обращенного в локальную сеть, выполняет роль шлюза по умолчанию для всех компьютеров, которым будет предоставлено право пользоваться ресурсами внешней сети.

Рассмотренный выше способ подключения локальной сети к сети более высокого порядка предусматривает ситуацию, при которой инициато-

рами соединения являются хосты внутренней сети. Но существует также вариант организации NAT, при котором происходит трансляция обращений к компьютеру локальной сети, имеющему внутренний IP-адрес и по умолчанию недоступному из Интернет. При этом осуществляется обратная замена в поле адреса назначения (Destination IP) в ответном пакете.

Такой механизм NAT, как правило, реализуется при помощи технологии PAT (Port Address Translation) – трансляции сетевых адресов в зависимости от TCP/UDP-порта получателя (рис. 3.40).

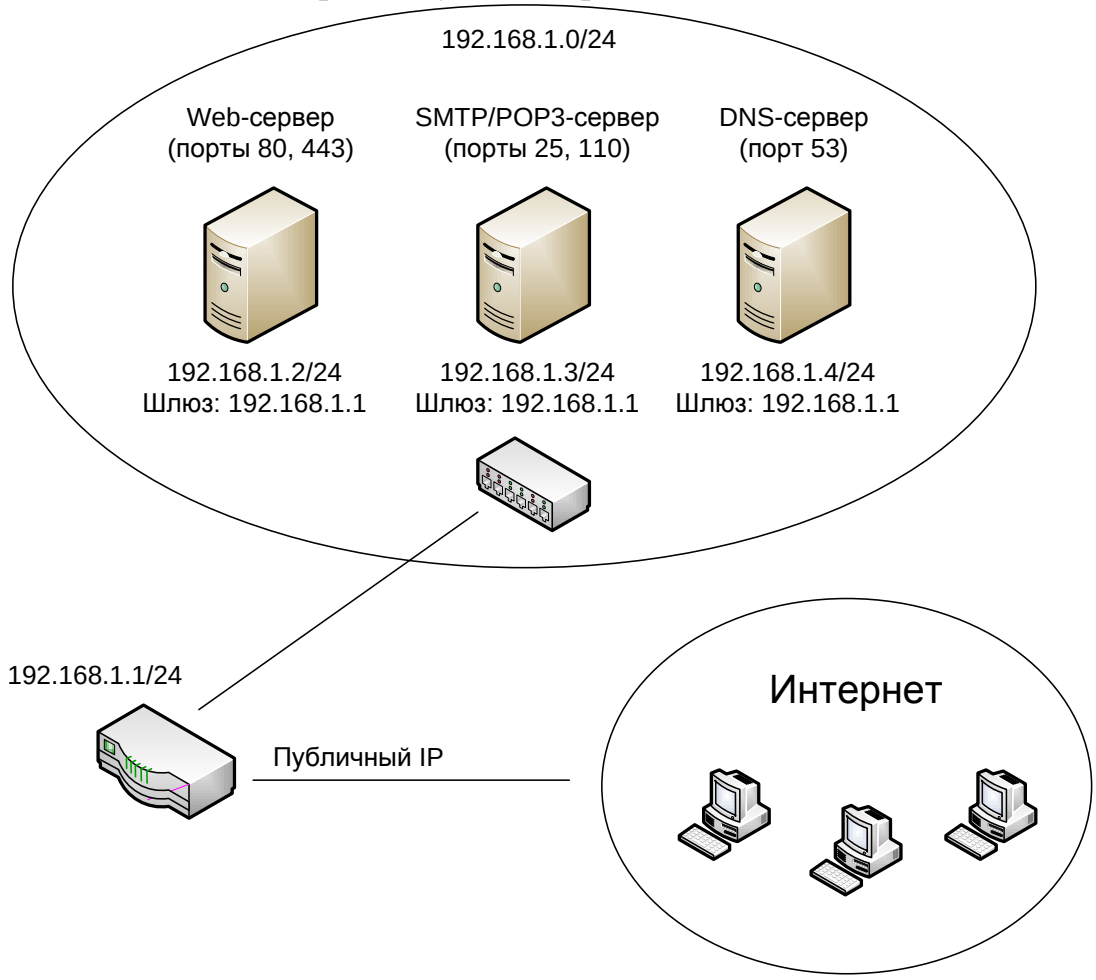


Рис. 3.40. Пример построения PAT

Маршрутизатор имеет два сетевых интерфейса: WAN (публичный IP-адрес, предоставленный провайдером), на который поступают запросы и для которого производится трансляция, LAN (192.168.1.1), который, в свою очередь, связан с серверами.

IP-пакеты, поступающие на маршрутизатор, в зависимости от адреса порта узла-получателя транслируются с различными адресами:

- порты 80 и 443 – Web-сервер (192.168.1.2);
- порты 25 и 110 – на SMTP/POP3-сервер (192.168.1.3);
- порт 53 – на DNS-сервер (192.168.1.4).

Ответы серверов транслируются через маршрутизатор с заменой адреса узла-отправителя.

На основании принципов построения NAT объединенную сеть принято разделять на два сегмента: NAT Inside (внутренняя) и NAT Outside (внешняя). У пакетов, приходящих из внешней сети, меняется адрес узла-получателя, у пакетов из внутренней сети происходит замена адреса узла-отправителя.

Как видно из рис. 3.40, NAT (а точнее, его разновидность – PAT) позволяет организовать доступ к ресурсам локальной сети из сети Интернет, используя при этом только один публичный IP-адрес, предоставленный провайдером. Таким образом, обеспечивается реальная экономия публичных IP-адресов.

В случае с обычным NAT, где хосты локальной сети не являются ресурсами, к которым требуется организовывать доступ из внешней сети, можно обойтись одним публичным адресом. В данном же примере (рис. 3.40) такие ресурсы – серверы развернуты во внутренней сети, и поставлена задача организации доступа к ним из внешней сети. Как показано выше, одним из эффективных решений данной задачи является организация трансляции сетевых адресов в зависимости от портов, используемых серверами.

3.17. Протокол IPv6

В конце прошлого века слала остро вырисовываться проблема нехватки в сети Интернет IP-адресов. Очевидно, что 32 бита, отведенные для поля адреса в протоколе IPv4, не способны в полной мере решать современные задачи высокоскоростных локальных и глобальных сетей. Вместе с тем исчерпание публичных адресов Интернет стало неизбежным. Была разработана новая версия протокола сетевого уровня IPv6, в котором для адреса отводилось уже не 32, а 128 бит.

Доля протокола IPv6 в сети Интернет по сравнению с IPv4 пока невелика из-за наличия в глобальной сети огромного количества узлов, которые просто не поддерживают IPv6 и, соответственно, являются устаревшими. Для них требуется предусмотреть механизмы специального преобразования, чтобы обеспечить интеграцию с узлами, использующими IPv6. Поэтому после исчерпания адресного пространства в IPv4, планируется параллельное использование двух стеков протоколов IPv6 и IPv4, с постепенным переходом с IPv4 на IPv6.

Общепринятая структура заголовка IP-пакета версии IPv6 (рис. 3.41) подробно описана в документе RFC 2460.

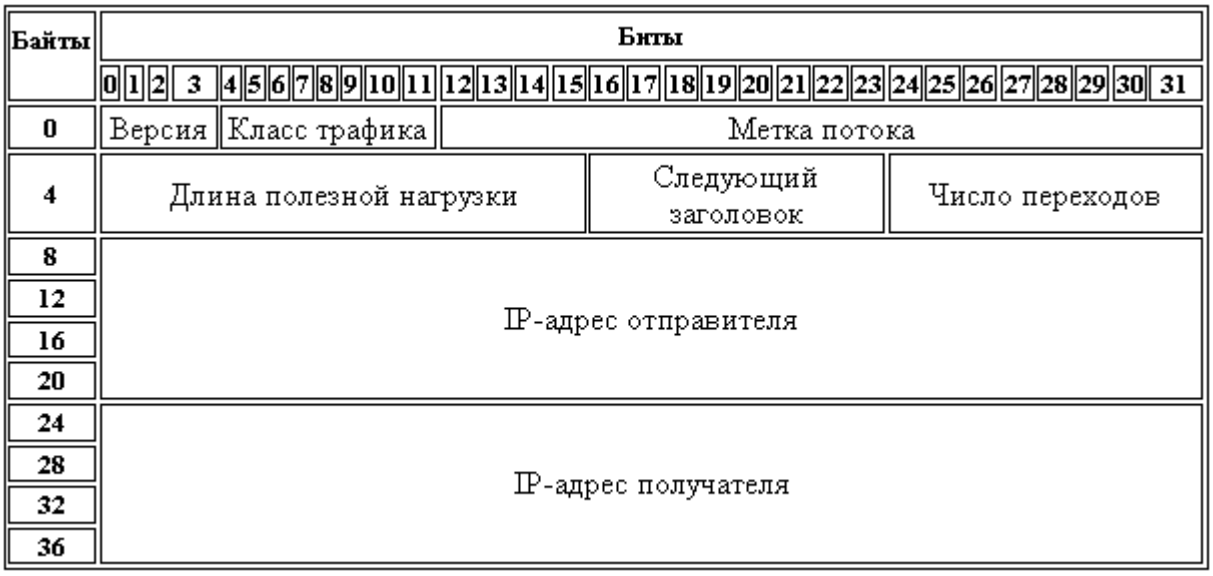


Рис. 3.41. Структура заголовка IPv6

- **Версия** – для IPv6 значение поля равно 6.
- **Класс трафика** – поле, на основании которого маршрутизаторы определяют приоритеты пакетов. Первые три бита определяют непосредственно класс трафика:
  0 – ничем не характеризующийся трафик;
  1 – сетевые новости;
  2 – электронная почта;
  3 – резерв;
  4 – HTTP, FTP, NFS;
  5 – резерв;
  6 – Telnet, SSH;
  7 – SNMP.

  Оставшиеся биты определяют приоритет удаления, чем больше это значение, тем выше приоритет пакета.
- **Метка потока** – уникальное значение, которое характеризует однородный поток пакетов, посылаемых узлом-отправителем узлу-получателю. Однородность пакетов в потоке определяется общими для них методами обработки, которые, в свою очередь, задаются дополнительными заголовками. Метка потока формируется узлом-отправителем путём генерации псевдослучайного числа длиной 20 бит. При этом все пакеты одного потока должны иметь одинаковые заголовки. Введение в протоколе IPv6 данного поля позволяет значительно упростить процедуру маршрутизации однородного потока пакетов в сети.
- **Длина полезной нагрузки** – длина поля данных в байтах без учета заголовка.

- **Следующий заголовок** – задаёт тип расширенного заголовка, который идёт следующим. В последнем расширенном заголовке данное поле задаёт тип протокола транспортного уровня (например, TCP или UDP).
- **Число переходов** – максимальное число маршрутизаторов, которые может пройти данный пакет. При прохождении маршрутизатора это значение уменьшается на единицу и когда становится равным 0, пакет отбрасывается.

Очевидным преимуществом протокола IPv6 по сравнению с IPv4 является, прежде всего, огромное адресное пространство, которое обеспечивается 128-битным полем адреса и позволяет не экономить IP-адреса, как это делалось при трансляции адресов в IPv4.

Вместе с тем необходимо подчеркнуть, что адресное пространство IPv6 было организовано с целью построения жесткой иерархии адресов, которая способна значительно упростить процедуру маршрутизации. Также применительно к маршрутизаторам из IPv6 по сравнению с IPv4 были исключены две важные функции:

1. Маршрутизаторы не участвуют в разбиении пакетов. Фрагментация IP-пакета осуществляется изначально на стороне хоста-отправителя, информация об этом вынесена из основного заголовка в расширенные;
2. В пакете IPv6 отсутствует поле контрольной суммы. Функция контроля целостности данных возложена на соседние уровни. Таким образом, маршрутизатору не приходится осуществлять процедуру пересчета контрольной суммы IP-пакета, когда тот проходит через него, уменьшая значение своего поля с числом переходов на единицу, как это было с TTL в IPv4.

Что касается пользовательских улучшений по сравнению с IPv4, то для IPv6 стоит отметить два заметных преимущества:

1. Применимость нового протокола для сверхскоростных сетей, где возможна передача информации при помощи огромных пакетов – до 4 Гигабайт;
2. Использование меток потоков и классов трафика, которые позволяют значительно улучшить показатели качества обслуживания.

3.18. Адресация в IPv6

Синтаксис IPv6 регламентирует запись адресов в шестнадцатиричной системе счисления. Таким образом, IP-адрес состоит из восьми групп по четыре цифры, которые разделены двоеточием, например, 2001:a8d9:4532:45b6:c793:ed62:00fc:4649.

Если одна или более групп подряд имеют вид 0000, то их принято заменять двойным двоеточием.

Например, адрес 2001:0000:0000:0000:0000:0000:dc65:6fd5 для удобства может быть записан в виде 2001::dc65:6fd5. Очевидно, что при таком подходе нельзя сокращать разделённые нулевые группы, это приведет к неоднозначности при восстановлении полноразмерного адреса.

Протокол IPv6 предполагает использование трех типов адресов:

Unicast – обычные адреса. Пакет, отправленный узлу с адресом такого типа, будет доставлен на его четко заданный интерфейс. Такие адреса делятся на категории:

- Глобальные – адреса, аналогичные публичным адресам IPv4. Могут находиться в любом не занятом диапазоне;
- Link-Local – адреса, аналогичные автосконфигурированным адресам IPv4 по протоколу APIPA: 169.254.0.0/16. Начинаются с цифры FE80;
- Unique-Local – адреса, аналогичные адресам IPv4 для построения частных локальных сетей: 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Начинаются с цифр FC00 и FD00, описаны в документе RFC 4193.

Anycast – адреса, которые используются исключительно маршрутизаторами. Пакет, отправленный узлу с адресом такого типа, попадёт на ближайший в соответствии с метрикой маршрутизатора интерфейс.

Multicast – адреса, характеризующие группу интерфейсов. Пакет, отправленный на такой адрес такого типа, будет доставлен всем интерфейсам, зарегистрированным в группе многоадресной рассылки.

Необходимо отметить, что используемые в IPv4 широковещательные адреса в IPv6 относятся именно к этому типу адресов.

Также необходимо учесть наличие в IPv6 зарезервированных адресов, которые не могут быть присвоены узлам сети (табл. 3.12).

Таблица 3.12

Адрес IPv6	Длина префикса, бит	Описание
::	128	Аналог 0.0.0.0 в IPv4
::1	128	loopback, аналог 127.0.0.1 в IPv4
::xx.xx.xx.xx	96	Последние 32 бита – адрес IPv4. Совместим с IPv6. Устарел
::ffff:xx.xx.xx.xx	96	Последние 32 бита – это адрес IPv4. Для хостов, не поддерживающих IPv6
2001:db8::	32	Зарезервирован для примеров в документации (RFC 3849)
fe80:: – febf::	10	Link-Local, аналог 169.254.0.0/16 в IPv4
fec0:: – feff::	10	Site-Local, аналог адресов IPv4: 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Устарел (RFC 3879)
fc00::	7	Unique-Local, аналог адресов IPv4: 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16
ffxx::	8	Multicast

Вопросы

1. Какие задачи решает протокол IP? Какие версии протокола IP существуют? В чем их различие?
2. Каким образом пакет IP связан с транспортным уровнем OSI?
3. Произведите подключение двух хостов с ОС Windows к локальной сети через коммутатор. Какие сетевые настройки необходимо произвести для обмена между ними информацией? Подсеть выбрать произвольно.
4. Можно ли компьютеру локальной сети назначить следующие IP-адреса: 192.168.1.1; 172.16.4.0; 225.1.1.5; 127.0.0.1; 10.10.5.6; 100.100.100.1? Если можно, то какие особенности необходимо учесть?
5. К каким подсетям принадлежат следующие IP-адреса: 10.1.1.1/24; 172.18.44.56/8; 192.168.100.0/16; 192.168.1.1/30?
6. Постройте таблицу всех адресов для подсети 192.168.90.0/28.
7. Каким образом хост-отправитель IP-пакетов в локальной сети определяет MAC-адрес хоста-получателя?
8. Для чего используется маршрутизация в локальных сетях?
9. Каковы основные отличия статической маршрутизации от динамической?
10. Какая информация содержится в таблице маршрутизации?
11. Какую роль выполняет шлюз по умолчанию для хостов в подсети?
12. Какие ограничения по структуре сети накладываются на протоколы RIP, EIGRP, OSPF?
13. В чем принцип работы алгоритма split horizon?
14. В чем различие между пограничными и магистральными маршрутизаторами при использовании OSPF?
15. Какой алгоритм нахождения кратчайшего пути используется в OSPF?
16. В чем состоит назначение протокола BGP?
17. Чем отличаются между собой unicast-трафик, broadcast-трафик и multicast трафик?
18. Приведите примеры локальных сетей, где имеет смысл использование multicast-вещания.
19. Для чего необходим контроль multicast-трафика в локальной сети, и какие устройства и протоколы для этого применяются?
20. Можно ли обойтись обычными протоколами (например, RIP) для маршрутизации multicast-трафика в локальной сети?
21. В чем состоит принцип трансляции адресов при сопряжении локальной сети и Интернета (NAT и PAT)?
22. В чем заключаются основные преимущества IPv6 перед IPv4?

Глоссарий

БДС (Блок Данных Службы) – это данные интерфейса уровня N, которые остаются неизменными от одной стороны соединения до другой.
ВОС – взаимодействие открытых систем.
ОС (Открытая Система) – открытой (Open System) называют систему, которая реализует открытые спецификации на интерфейсы, услуги и форматы данных.
ОТС (Оконечная Точка Соединения) – элемент ТДС, являющийся частью соединения уровня N.
ПО – программное обеспечение.
ПП (Прикладной Процесс) – ведет обработку данных для некоторого приложения (решая пользовательскую задачу).
РОС (Реальная Открытая Система) – это система, которая удовлетворяет требованиям ITU-T X.200 (ISO 7498) при ее взаимодействии с другими РС.
РС – реальная система.
Служба – комплекс аппаратных и программных средств сети связи, а также поддерживающих их средств технической эксплуатации, технического обслуживания и административного управления, которые обеспечивают предоставление услуг пользователю.
ССОП (Сеть Связи Общего Пользования) – предназначена для предоставления услуг электросвязи любому пользователю на территории Российской Федерации.
ТфОП (Телефонная сеть общего пользования) (PSTN, Public Switched Telephone Network) — это сеть, для доступа к которой используются обычные проводные телефонные аппараты, мини-АТС и оборудование передачи данных.
ТДС (Точка Доступа к Службе) – точка, в которой данный уровень предоставляет услуги уровню (N +1).
ЭМВОС – эталонная модель взаимодействия открытых систем.
802.1Q — стандарт VLAN на базе тега.
AC (Alternate Current) — переменный ток.
BPDU (Bridge Protocol Data Unit) — кадр, используемый протоколом STP/RSTP при построении дерева.
CLI (Command Line Interface) — интерфейс командной строки.
DA (Destination Address) — адрес назначения.
DSCP (DiffServ Code Point) — 6-битовое поле в заголовке IP-пакета, обычно используется для приоритезации.
DVMRP (Distance Vector Multicast Routing Protocol) — дистанционно-векторный протокол маршрутизации групповых рассылок (RFC 1075).
EAP (Extensible Authentication Protocol) — расширяемый протокол аутентификации. Известные расширения этого протокола: EAP-MD5, EAP-TLS (со взаимной аутентификацией сторон с помощью сертификатов) и

EAP-TTLS (с аутентификацией сервера на основе сертификата и аутентификацией клиента по логину и паролю).
FCS (Frame Check Sum) — контрольная сумма кадра.
GARP (Generic Attribute Registration Protocol) — протокол общего назначения для регистрации атрибутов.
GUI (Graphical User Interface) — графический интерфейс пользователя, например web-браузер.
GVRP (GARP VLAN Registration Protocol) — протокол динамической регистрации VLAN, основанный на GARP.
HDAP (Host Discovery and Address assignment Protocol) — протокол для обнаружения узла и назначения адреса, используется устройствами ZyXEL для централизованного управления iStacking.
IGMP (Internet Group Management Protocol) — протокол управления группами многоадресных рассылок (RFC 1112, RFC 2236, RFC 3376).
L/T (Length/Type) — поле Типа/Длины кадра Ethernet.
LACP (Link Aggregation Control Protocol) — протокол управления агрегированными каналами.
MAC (Media Access Control) — управление доступом к среде.
MAC-адрес — адрес устройства в локальной сети.
MSTP (Multiple Spanning Tree Protocol) — алгоритм покрывающего дерева, работающий внутри VLAN. VLAN в сети может быть несколько, отсюда и название алгоритма (IEEE 802.1s).
MRSTP (Multiple RSTP) — реализация RSTP в некоторых коммутаторах ZyXEL, позволяющая включать один коммутатор в несколько деревьев RSTP. Для этого на коммутаторе указываются группы портов, относящихся к различным экземплярам RSTP.
MTU (Maximum Transfer Unit) — максимальный размер пакета, допустимый к передаче в данном сегменте локальной сети.
MVR (Multicast VLAN Registration) — метод отправки групповых рассылок в отдельном VLAN.
NAT (Network Address Translation) — механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса проходящих пакетов (RFC 1631, RFC 3022).
NAPT (Network Address Port Translation) — частный случай механизма NAT, который помимо подмены IP-адресов проходящих пакетов обеспечивает подмену TCP/UDP портов проходящих пакетов (RFC 3022).
OSPF (Open Shortest Path First) — протокол маршрутизации (RFC 2328).
PEAP (Protected Extensible Authentication Protocol) — защищенный расширяемый протокол аутентификации. Приблизительно тоже самое, что EAP-TTLS, инициатива Microsoft и Cisco.
QoS (Quality of Service) — качество обслуживания.

RADIUS (Remote Authentication Dial-In User Service) — служба, отвечающая за аутентификацию пользователей. На сервере RADIUS хранится информация о пользователях и паролях (RFC 2865, RFC 2866).
RIP (Routing Information Protocol) — дистанционно-векторный маршрутизирующий протокол. Из-за медленной сходимости применяется только в небольших сетях (RFC 1058, RFC 2453).
RFC (Request For Comment) — общее название документа-рекомендации комитета IETF (Internet Engineering Task Force).
RSTP (Rapid Spanning Tree Protocol) — улучшенная редакция протокола STP с быстрым восстановлением связности сети при разрывах в активной топологии (IEEE 802.1w).
SA (Source Address) — адрес источника.
SFP (Small Factor Pluggable) — универсальный модуль для подключения оптоволоконного канала к коммутатору.
SPQ (Strict Priority Queueing) — алгоритм обработки очередей на порту коммутатора.
STP (Spanning Tree Protocol) — протокол покрывающего дерева, служит для удаления циклов из сети (IEEE 802.1d).
TCI (Tag Control Information) — управляющая информация, содержащаяся в теге 802.1Q.
TOS (Type of Service) — флаговое поле в заголовке IP-пакета. Флаги отвечают за тип обслуживания - «наилучшее время», «наименьшая стоимость» и т.п.
TPID (Tag Protocol Identifier) — идентификатор протокола тега (маркера) 802.1Q.
VID (VLAN Identifier) — идентификатор VLAN.
VLAN (Virtual Local Area Network) — виртуальная локальная сеть.
VRRP (Virtual Router Redundancy Protocol) — протокол виртуального отказоустойчивого маршрутизатора (RFC 3768).
WDM (Wavelength Division Multiplexing) — метод полнодуплексной передачи данных по одному оптоволоконному кабелю, когда прямой и обратный сигналы передаются на различных длинах волн.
WFQ (Weighted Fair Queuing) — алгоритм управления «взвешенными» очередями пакетов, основан на весах очередей и объеме отправляемых данных.
WRR (Weighted Round Robin) — простой циклический алгоритм управления «взвешенными» очередями пакетов, основан на весах очередей и количестве отправляемых пакетов.

Литература

1) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. Издание 4-ое / СПб: Изд-во «Питер», 2010.
2) Дуглас Э. Камер С. Сети TCP/IP. Принципы, протоколы и структура. Том 1. Издание 4-ое. Издательский дом «Вильямс». Москва – С-Петербург – Киев, 2003.
3) Столингс В. Компьютерные сети, протоколы и технологии Интернет. – СПб. БХВ-Петербург, 2005.
4) Жигадло В.Э., Бородко А.В. Архитектура протоколов и сетевые возможности операционной системы Windows: учеб. пособие / СПбГУТ. СПб, 2007.
5) Небаев И.А. Конфигурирование и управление маршрутизаторами на основе интерфейса командной оболочки Cisco IOS. учеб. пособие / СПб ГУТ. СПб, 2012 г.

Бородко Александр Владимирович
Кукунин Дмитрий Сергеевич

КОМПЬЮТЕРНЫЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ
Часть 1

Редактор

План 2013 г., п. 11

Подписано к печати 1.05.2013
Объем 12,75 усл.-печ. л. Тираж экз. Заказ

Издательство СПбГУТ. 191186 СПб., наб. р. Мойки, 61
Отпечатано в