ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.14 Сети и телекоммуникации

(*код и наименование дисциплины в соответствии с РУП*)

Направление подготовки (специальность) 09.03.01 «Информатика и вычислительная техника»

Профиль образовательной программы «Автоматизированные системы обработки информации и управления**»**

Форма обучения *очная*

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1.1 Лекция №1 (2 часа).

Тема: «Общие сведения о компьютерных сетях»

1.1.1 Вопросы лекции:

1. Классификация сетей.

2. Топология сетей.

1.1.2 Краткое содержание вопросов:

1. Классификация сетей.

Классификация сетей ЭВМ (компьютерных сетей), как любых больших и сложных систем, может быть выполнена на основе различных признаков, в качестве которых могут быть использованы (рис.1):

- размер (территориальный охват) сети;
- принадлежность;
- назначение;
- область применения.

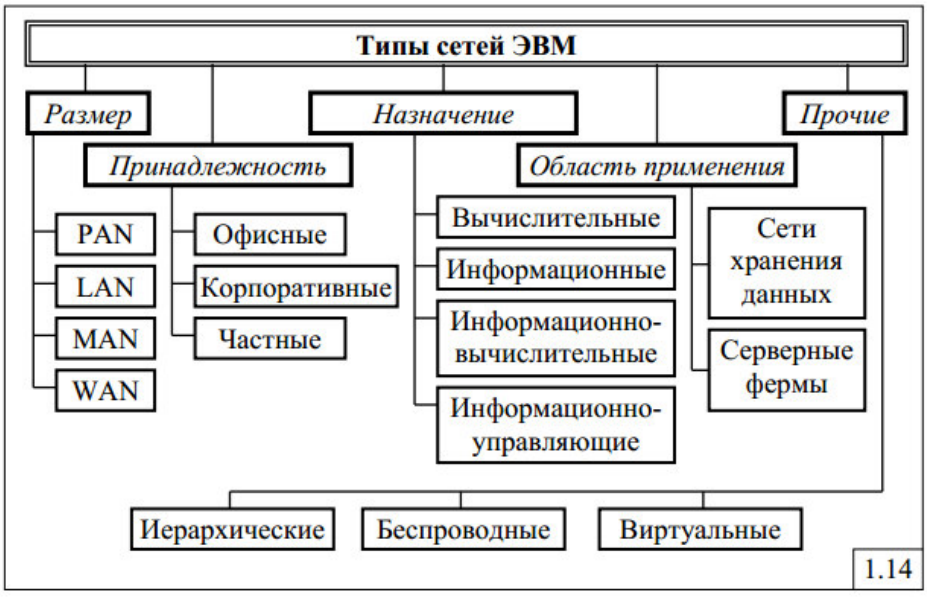


Рисунок 1.Типы сетей ЭВМ

1. **По размеру (территориальному охвату)** сети ЭВМ делятся на:

- персональные;
- локальные;
- городские (региональные).
- глобальные.

Персональная сеть (PersonalAreaNetwork, PAN) — это сеть,объединяющая персональные электронные устройства пользователя (телефоны, карманные персональные компьютеры, смартфоны, ноутбуки и т.п.) и характеризующаяся:

- небольшим числом абонентов;
- малым радиусом действия (до нескольких десятков метров);
- некритичностью к отказам.

К стандартам таких сетей в настоящее время относятся Bluetooth, Zigbee, Пиконет.

Локальная вычислительная сеть (ЛВС) (LocalAreaNetwork, LAN)– сеть со скоростью передачи данных , как правило, не менее 1 Мбит/с, обеспечивающая связь на небольших расстояниях – от нескольких десятков метров до нескольких километров. Оборудование, подключаемое к ЛВС, может находиться в одном или нескольких соседних зданиях.

ПримерыЛВС: Ethernet, Token Ring.

Городская вычислительная сеть (MetropolitanAreaNetwork, MAN) – сеть, промежуточная по размеру между ЛВС и глобальной сетью.

Протоколы и кабельная система для городской вычислительной сети описываются в стандартах комитета IEEE 802.6. MAN реализуется на основе протокола DQDB (DistributedQueueDualBus) – двойная шина сраспределенной очередью и использует волоконно-оптический кабель для передачи данных со скоростью 100 Мбит/с на территории до 100 км2. MAN может применяться для объединения в одну сеть группы сетей, расположенных в разных зданиях. Последние разработки, связанные с высокоскоростным беспроводным доступом в соответствии со стандартом IEEE 802.16, привели к созданию MAN в виде широкополосных беспроводных ЛВС.

Глобальная сеть (WideAreaNetwork, WAN) – в отличие от ЛВС охватывает большую территорию и представляет собой объединение нескольких ЛВС, связанных с помощью специального сетевого оборудования (маршрутизаторов, коммутаторов и шлюзов), образующих в случае использования высокоскоростных каналов магистральную сеть передачи данных (магистральную сеть связи). Наиболее широкое применение находят глобальные сети для нужд информационного обмена в коммерческих, научных и других профессиональных целях.

Для построения глобальных сетей могут использоваться различные сетевые технологии, в том числе TCP/IP, X.25, FrameRelay, ATM, MPLS.

Настоящей глобальной сетью, пожалуй, можно считать только сеть Интернет. Вряд ли глобальной можно считать сеть, объединяющую 2-3 ЛВС, находящиеся в разных городах, расположенных на расстоянии нескольких десятков или даже сотен километров

друг от друга. Однако, поскольку для построения такой «простой» сети используются обычно те же сетевые технологии и технические средства, что и в сети Интернет, то такие сети обычно тоже относят к классу глобальных сетей.

2. **По принадлежности** сети ЭВМ делятся на:

- офисные – сети, расположенные на территории офиса компании, ограниченной обычно пределами одного здания, и построенные на технологиях LAN;
- корпоративные (ведомственные) – сети, представляющие собой объединение нескольких офисных сетей компании, расположенных в разных территориально разнесенных зданиях, находящихся возможно в разных городах и регионах, и построенные на технологиях MAN или WAN;
- частные – сети, построенные обычно на технологии виртуальной частной сети (VirtualPrivateNetwork, VPN), позволяющей обеспечить одно или несколько сетевых соединений, которые могут быть трёх видов: узел-узел, узел-сеть и сеть-сеть, образующих логическую сеть поверхдругой сети (например, Интернет).

3. **По назначению** сети ЭВМ делятся на:

- вычислительные, предназначенные для решения задач пользователей, ориентированных, в основном, на вычисления;
- информационные, ориентированные на предоставление информационных услуг; примерами таких сетей могут служить сети, предоставляющие справочные и библиотечные услуги.

2. Топология сетей.

Термин ***топология сети*** означает способ соединения компьютеров в сеть. Вы также можете услышать другие названия – ***структура сети*** или***конфигурация сети*** (это одно и то же). Кроме того, понятие топологии включает множество правил, которые определяют места размещения компьютеров, способы прокладки кабеля, способы размещения связующего оборудования и многое другое. На сегодняшний день сформировались и устоялись несколько основных топологий. Из них можно отметить “**шину**”, “**кольцо**” и “**звезду**”.

Топология “шина”

Топология ***шина*** (рис.2) (или, как ее еще часто называют ***общая шина*** или ***магистраль***) предполагает использование одного кабеля, к которому подсоединены все рабочие станции.

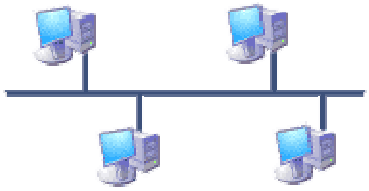


Рисунок 2. Топология шина.

Общий кабель используется всеми станциями по очереди. Все сообщения, посылаемые отдельными рабочими станциями, принимаются и прослушиваются всеми остальными компьютерами, подключенными к сети. Из этого потока каждая рабочая станция отбирает адресованные только ей сообщения.

Достоинства топологии “шина”:

- простота настройки;
- относительная простота монтажа и дешевизна, если все рабочие станции расположены рядом;
- выход из строя одной или нескольких рабочих станций никак не отражается на работе всей сети.

Недостатки топологии “шина”:

- неполадки шины в любом месте (обрыв кабеля, выход из строя сетевого коннектора) приводят к неработоспособности сети;
- сложность поиска неисправностей;
- низкая производительность – в каждый момент времени только один компьютер может передавать данные в сеть, с увеличением числа рабочих станций производительность сети падает;
- плохая масштабируемость – для добавления новых рабочих станций необходимо заменять участки существующей шины.

Именно по топологии “шина” строились локальные сети на коаксиальном кабеле. В этом случае в качестве шины выступали отрезки коаксиального кабеля, соединенные Т-коннекторами. Шина прокладывалась через все помещения и подходила к каждому компьютеру. Боковой вывод Т-коннектора вставлялся в разъем на сетевой карте. Сейчас такие сети безнадежно устарели и повсюду заменены “звездой” на витой паре, однако оборудование под коаксиальный кабель еще можно увидеть на некоторых предприятиях.

Топология “кольцо”

Кольцо – это топология локальной сети, в которой рабочие станции подключены последовательно друг к другу, образуя замкнутое кольцо. Данные передаются от одной рабочей станции к другой в одном направлении (по кругу) (рис.3). Каждый ПК работает как повторитель, ретранслируя сообщения к следующему ПК, т.е. данные передаются от одного компьютера к другому как бы по эстафете.

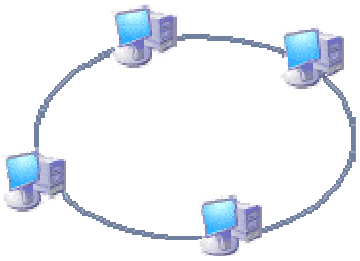


Рисунок 3. Топология кольцо.

Если компьютер получает данные, предназначенные для другого компьютера – он передает их дальше по кольцу, в ином случае они дальше не передаются.

Достоинства кольцевой топологии:

- простота установки;
- практически полное отсутствие дополнительного оборудования;
- возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети.

Однако “кольцо” имеет и существенные недостатки:

- каждая рабочая станция должна активно участвовать в пересылке информации; в случае выхода из строя хотя бы одной из них или обрыва кабеля – работа всей сети останавливается;
- подключение новой рабочей станции требует краткосрочного выключения сети, поскольку во время установки нового ПК кольцо должно быть разомкнуто;
- сложность конфигурирования и настройки;
- сложность поиска неисправностей.

Кольцевая топология сети используется довольно редко. Основное применение она нашла в оптоволоконных сетях стандарта TokenRing.

Топология “звезда”

Звезда – это топология локальной сети, где каждая рабочая станция присоединена к центральному устройству (коммутатору или маршрутизатору) (рис.4). Центральное устройство управляет движением пакетов в сети. Каждый компьютер через сетевую карту подключается к коммутатору отдельным кабелем.

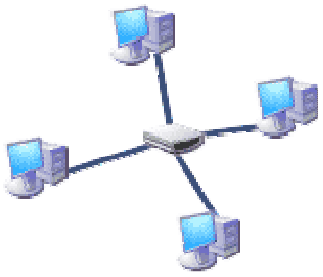


Рисунок 4. Топология звезда.

При необходимости можно объединить вместе несколько сетей с топологией “звезда” – в результате вы получите конфигурацию сети с ***древовидной*** топологией. Древовидная топология распространена в крупных компаниях. Мы не будем ее подробно рассматривать в данной статье.

Топология “звезда” на сегодняшний день стала основной при построении локальных сетей. Это произошло благодаря ее многочисленным достоинствам:

- выход из строя одной рабочей станции или повреждение ее кабеля не отражается на работе всей сети в целом;
- отличная масштабируемость: для подключения новой рабочей станции достаточно проложить от коммутатора отдельный кабель;
- легкий поиск и устранение неисправностей и обрывов в сети;
- высокая производительность;
- простота настройки и администрирования;
- в сеть легко встраивается дополнительное оборудование.
-

Однако, как и любая топология, “звезда” не лишена недостатков:

- выход из строя центрального коммутатора обернется неработоспособностью всей сети;
- дополнительные затраты на сетевое оборудование – устройство, к которому будут подключены все компьютеры сети (коммутатор);
- число рабочих станций ограничено количеством портов в центральном коммутаторе.

Звезда – самая распространенная топология для проводных и беспроводных сетей. Примером звездообразной топологии является сеть с кабелем типа витая пара, и коммутатором в качестве центрального устройства. Именно такие сети встречаются в большинстве организаций.

1.2 Лекция №2 (2 часа).

Тема: «Коммутация»

1.2.1 Вопросы лекции:

1. Способы коммутации.
2. Разделение каналов по времени.
3. Разделение каналов по частоте.

1.2.2 Краткое содержание вопросов:

1. Способы коммутации.

Пакеты в сети могут передаваться двумя способами (рис.5):

- дейтаграммным;
- путем формирования «виртуального канала».

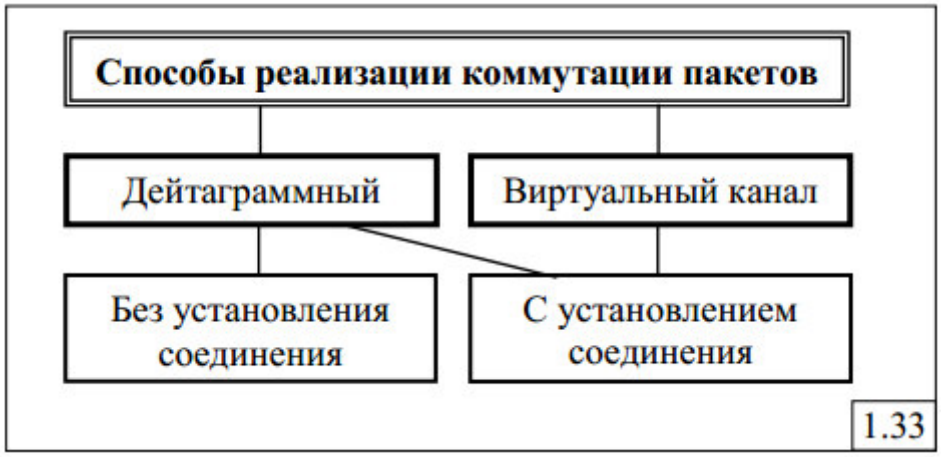


Рисунок 5. Способы реализации коммутации.

При **дейтаграммном** способе пакеты одного и того же сообщения могут передаваться между двумя взаимодействующими пользователями А и В по разным маршрутам, как это показано на рис.6, где пакет П1 передаётся по маршруту У1-У2-У6-У7, пакет П2 – по маршруту У1-У4-У7 и пакет П3 – по маршруту У1-У3-У5-У7.

В результате такого способа передачи все пакеты приходят в конечный узел сети в разное время и в произвольной последовательности. Пакеты одного и того же сообщения, рассматриваемые в каждом узле сети как самостоятельные независимые единицы данных

и передаваемые разными маршрутами, называются дейтаграммами (datagram). В узлах сети для каждой дейтаграммы всякий раз определяется наилучший путь передачи в соответствии с выбранной метрикой маршрутизации, не зависимо от того, по какому пути переданы были предыдущие дейтаграммы с такими же адресами назначения (получателя) и источника (отправителя).

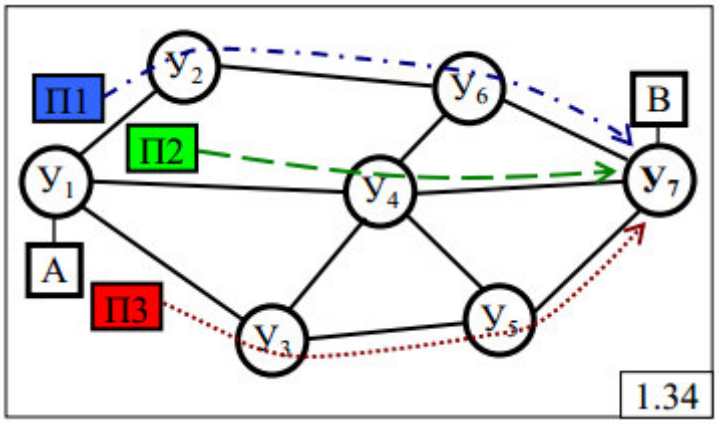


Рисунок 6. Дейтаграммный способ.

Дейтаграммный способ передачи пакетов может быть реализован:

- без установления соединения между абонентами сети;
- с установлением соединения между взаимодействующими абонентами сети.

В последнем случае между взаимодействующими абонентами предварительно устанавливается соединение путём обмена служебными пакетами: «запрос на соединение» и «подтверждение соединения», означающее готовность принять передаваемые данные. В процессе установления соединения могут «оговариваться» значения параметров передачи данных, которые должны выполняться в течение сеанса связи. После установления соединения отправитель начинает передачу, причём пакеты одного и того же сообщения могут передаваться разными маршрутами, то есть дейтаграммным способом. По завершении сеанса передачи данных выполняется процедура разрыва соединения путём обмена служебными пакетами: «запрос на разрыв соединения» и «подтверждение разрыва соединения». Описанная процедура передачи пакетов с установлением соединения иллюстрируется на диаграмме (рис.7).

Достоинствами дейтаграммного способа передачи пакетов в компьютерных сетях являются:

- простота организации и реализации передачи данных – каждый пакет (дейтаграмма) сообщения передаётся независимо от других пакетов;
- в узлах сети для каждого пакета выбирается наилучший путь (маршрут);

• передача данных может выполняться как без установления соединения между взаимодействующими абонентами, так и при необходимости с установлением соединения.

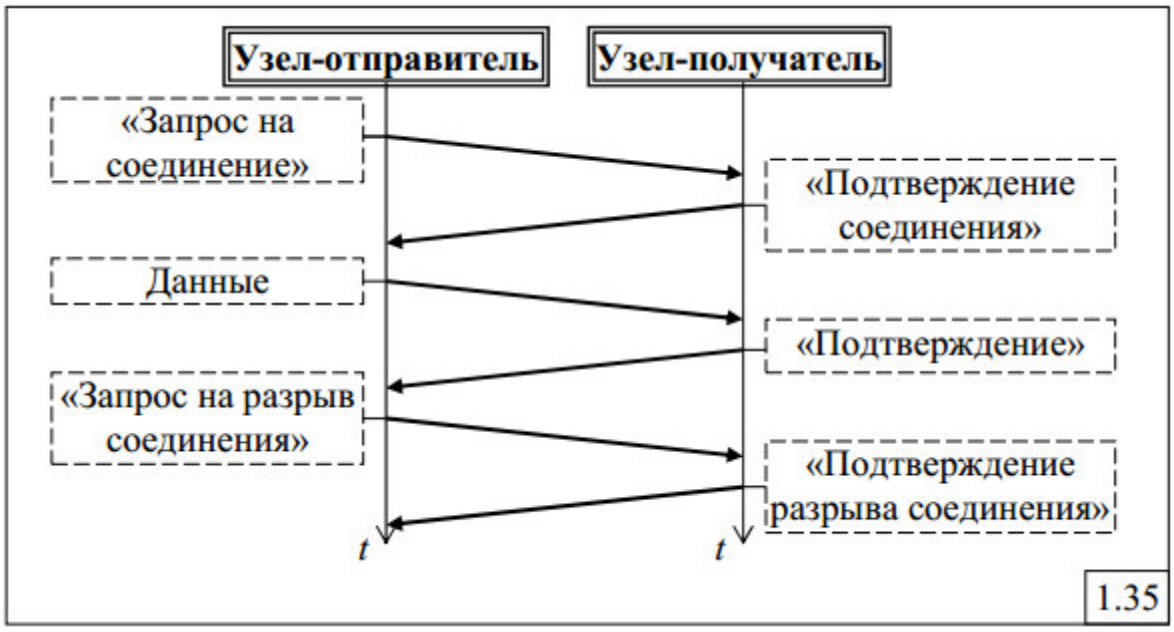


Рисунок 7. Процедура передачи пакетов

К недостаткам дейтаграммного способа передачи пакетов следует отнести:

• необходимость сборки сообщения в конечном узле: сообщение не может быть передано получателю, пока в конечном узле сети не соберутся все пакеты данного сообщения, поэтому в случае потери хотя бы одного пакета сообщение не сможет быть сформировано и передано получателю;

• при длительном ожидании пакетов одного и того же сообщения в конечном узле может скопиться достаточно большое количество пакетов сообщений, собранных не полностью, что требует значительных затрат на организацию в узле буферной памяти большой ёмкости;

• для предотвращения переполнения буферной памяти узла время нахождения (ожидания) пакетов одного и того же сообщения в конечном узле ограничивается, и по истечении этого времени все поступившие пакеты не полностью собранного сообщения уничтожаются, после чего выполняется запрос на повторную передачу данного сообщения; это приводит к увеличению нагрузки на сеть и, как следствие, к снижению её производительности, измеряемой количеством сообщений, передаваемых в сети за единицу времени.

Способ передачи пакетов «**виртуальный канал**» заключается в формировании единого «виртуального» канала на время взаимодействия абонентов для передачи всех

пакетов сообщения. Этот способ реализуется с использованием предварительного установления соединения между взаимодействующими абонентами, в процессе которого формируется наиболее рациональный единый для всех пакетов маршрут, по которому, в отличие от дейтаграммного способа, все пакеты сообщения передаются в естественной последовательности, как это показано на рис.8.

Пакеты П1, П2 и П3 сообщения передаются в естественной последовательности от пользователя А к пользователю В по предварительно созданному виртуальному каналу через узлы У1-У4-У7.

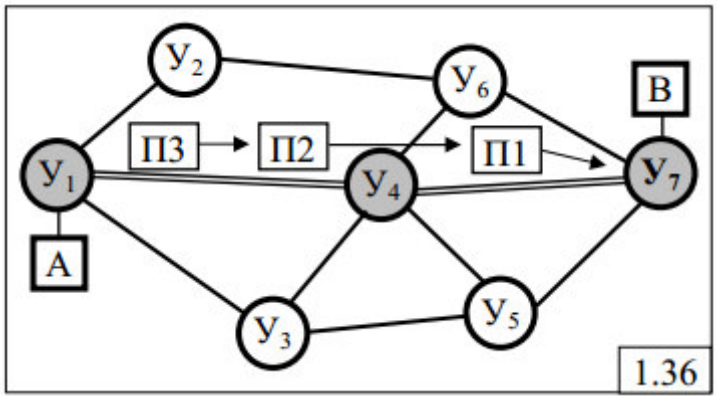


Рисунок 8. Передача пакетов сообщения.

Виртуальный канал, как и реальный физический канал в случае коммутации каналов, существует только в течение сеанса связи, при этом ресурсы реальных каналов связи (пропускная способность) и узлов сети (буферная память), находящихся на маршруте, резервируются на всё время сеанса.

Не следует путать и смешивать коммутацию каналов и способ передачи пакетов «виртуальный канал». Основное их отличие состоит в том, что «виртуальной канал» реализуется с промежуточным хранением пакетов в узлах сети, в то время как коммутация каналов реализуется без промежуточного хранения передаваемых пакетов за счёт создания реального (а не виртуального) физического канала между абонентами сети.

К достоинствам способа передачи пакетов «виртуальный канал» по сравнению с дейтаграммной передачей пакетов можно отнести:

- меньшие задержки в узлах сети, обусловленные резервированием ресурсов, и прежде всего пропускной способности каналов связи, в процессе установления соединения;

- небольшое время ожидания в конечном узле для сборки всего сообщения, поскольку пакеты передаются последовательно друг за другом по одному и тому же маршруту (виртуальному каналу), и вероятность того, что какой-либо пакет «заблудится» в результате неудачно выбранногомаршрута или его время доставки окажется слишком большим, как это может произойти при дейтаграммном способе, близка к нулю;
- более эффективное использование буферной памяти промежуточных узлов за счёт её предварительного резервирования, а также буферной памяти в конечном узле в связи с небольшим временем ожидания прихода всех пакетов сообщения.

К недостаткам способа передачи пакетов «виртуальный канал» можно отнести:

- наличие накладных расходов (издержек) на установление соединения;
- неэффективное использование ресурсов сети, поскольку они резервируются на всё время взаимодействия абонентов (сеанса) и не могут быть предоставлены другому соединению, даже если они в данный момент не используются.

2. Разделение каналов по времени.

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны быть высокоскоростными и поддерживать какую-либо технику мультиплексирования абонентских каналов. В настоящее время для мультиплексирования абонентских каналов используются две техники: техника частотного мультиплексирования (Frequency Division Multiplexing, FDM); техника мультиплексирования с разделением времени (Time Division Multiplexing, TDM).

Коммутация каналов на основе частотного мультиплексирования

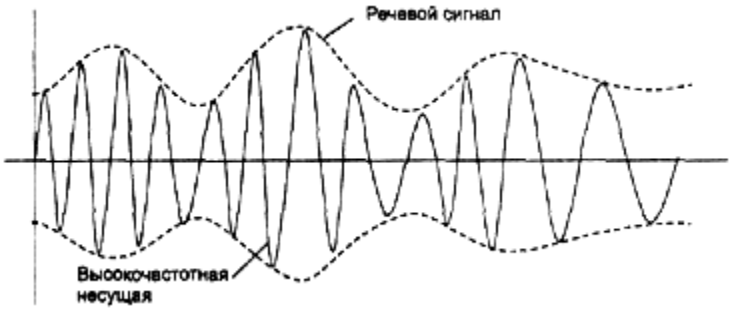


Рисунок 9. Модуляция речевых сигналов

Техника частотного мультиплексирования каналов (FDM) была разработана для телефонных сетей, но применяется она и для других видов сетей, например сетей кабельного телевидения.

Для разделения абонентских каналов характерна техника модуляции высокочастотного несущего синусоидального сигнала низкочастотным речевым сигналом (рис. 9). Если сигналы каждого абонентского канала перенести в свой собственный диапазон частот, то в одном широкополосном канале можно одновременно передавать сигналы нескольких абонентских каналов. На входы FDM- коммутатора поступают исходные сигналы от абонентов телефонной сети. Коммутатор выполняет перенос частоты каждого канала в свой диапазон частот. Обычно высокочастотный диапазон делится на полосы, которые отводятся для передачи данных абонентских каналов. Такой канал называют уплотненным. Коммутаторы FDM могут выполнять как динамическую, так и постоянную ком¬мутацию. При динамической коммутации один абонент инициирует соединение с другим абонентом, посылая в сеть номер вызываемого абонента. Коммутатор дина¬мически выделяет данному абоненту одну из свободных полос своего уплотненно¬го канала. При постоянной коммутации за абонентом полоса закрепляется на длительный срок путем настройки коммутатора по отдельному входу, недоступ¬ному пользователям. Коммутация каналов на основе разделения времени разрабатывалась в расчете на передачу непрерывных сигналов, представляющих голос. При переходе к цифро¬вой форме представления голоса была разработана новая техника мультиплекси¬рования, ориентирующаяся на дискретный характер передаваемых данных. Эта техника носит название мультиплексирования с разделением времени (Time Division Multiplexing, TDM). Реже используется и другое ее название — техника синхронного режима передачи (Synchronous Transfer Mode, STM). Аппаратура TDM-сетей — мультиплексоры, коммутаторы, демультиплексоры — работает в режиме разделения времени, поочередно обслуживая в течение цикла своей работы все абонентские каналы. Цикл работы оборудования TDM равен 125 мкс, что соответствует периоду следования замеров голоса в цифровом абонентском канале. Это значит, что мультиплексор или коммутатор успевает вовремя обслужить любой абонентский канал и передать его очередной замер далее по сети. Каждому соединению выделяется один квант времени цикла работы аппаратуры, называемый также тайм-слотом. Длительность тайм-слота зависит от числа абонентских каналов, обслуживаемых мультиплексором TDM или коммутатором. Мультиплексор принимает информацию по N входным каналам от конечных абонентов, каждый из которых передает данные по абонентскому каналу со скоростью 64 Кбит/с — 1 байт каждые 125 мкс. В каждом цикле мультиплексор

выполняет следующие действия: прием от каждого канала очередного байта данных; составление из принятых байтов уплотненного кадра, называемого также обоймой; передача уплотненного кадра на выходной канал с битовой скоростью, равной Nx64 Кбит/с. Порядок байт в обойме соответствует номеру входного канала, от которого этот байт получен. Количество обслуживаемых мультиплексором абонентских каналов зависит от его быстродействия. Демультиплексор выполняет обратную задачу — он разбирает байты уплотненного кадра и распределяет их по своим нескольким выходным каналам, при этом он считает, что порядковый номер байта в обойме соответствует номеру выходного канала.

Коммутатор принимает уплотненный кадр по скоростному каналу от мульти¬плексора и записывает каждый байт из него в отдельную ячейку своей буферной памяти, причем в том порядке, в котором эти байты были упакованы в уплотненный кадр. Для выполнения операции коммутации байты извлекаются из буферной памяти не в порядке поступления, а в таком порядке, который соответствует под¬держиваемым в сети соединениям абонентов.

Развитием идей статистического мультиплексирования стала технология асинхронного режима передачи — ATM, которая вобрала в себя лучшие черты техники коммутации каналов и пакетов.

3.Разделение каналов по частоте

Частотное разделение каналов (ЧРК) — разделение каналов по частоте, при котором каждому каналу выделяется определённый диапазон частот. В многоканальных системах связи (МКС) с ЧРК канальные сигналы отличаются друг от друга положением своих спектров на оси частот. Обычно системы с ЧРК используются для передачи аналоговых сигналов. На рис. 10 представлена структурная схема простейшей МКС с ЧРК.

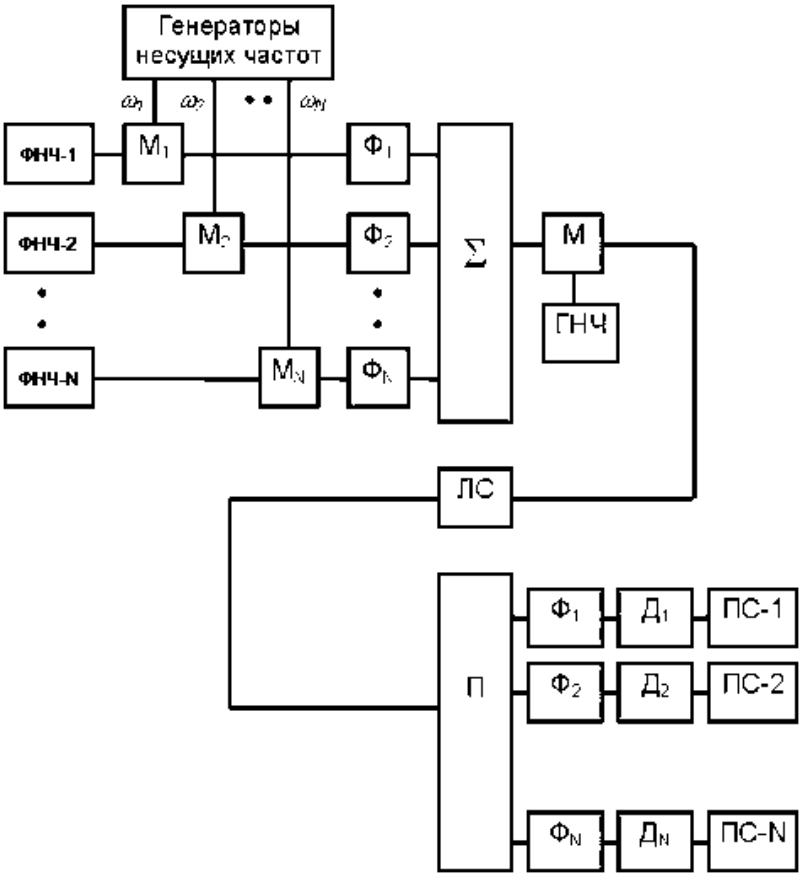


Рисунок 10. Структурная схема многоканальной системы с ЧРК

Наиболее часто в отдельных каналах при ЧРК применяется однополосная модуляция с соответственно подобранными частотами пилот-сигналов, которые выдаются генератором несущих частот (ГНЧ). Данный способ модуляции обеспечивает минимальную полосу частот группового сигнала. Подавление несущих достигается в индивидуальных модуляторах ($М_1$, $М_2$. ... $М_N$), которые, как правило, строятся по балансной схеме, а выделение одной боковой полосы (ОБП) осуществляется в полосовых фильтрах ($Ф_1$, $Ф_2$, ... $Ф_N$). Совокупность канальных сигналов на выходе суммирующего устройства Σ образует групповой сигнал. В групповом передатчике М групповой сигнал преобразуется в линейный сигнал, который и поступает в линию связи ЛС.

На приемной стороне линии связи линейный сигнал с помощью группового приемника П вновь преобразуется в групповой сигнал, из которого полосовыми фильтрами ($Ф_1$, $Ф_2$, ... $Ф_N$) выделяются канальные сигналы. После детектирования в канальных демодуляторах ($Д_1$, $Д_2$, ... $Д_N$) сигналы преобразуются в предназначенные получателям сообщения приемниками сообщений ($ПС_1$, $ПС_2$, ... $ПС_N$). Опорные колебания в канальных демодуляторах создаются с помощью генератора (ГНЧ). Сообщения, передаваемые по различным каналам, выделяются при помощи ФНЧ. .

Канальные передатчики вместе с суммирующим устройством образуют аппаратуру объединения. Групповой передатчик М, линия связи ЛС и групповой приемник П составляют групповой канал связи (тракт передачи), который вместе с аппаратурой объединения и индивидуальными приемниками составляет систему многоканальной связи. В составе технических устройств на передающей стороне многоканальной системы должна быть предусмотрена аппаратура объединения, а на приемной стороне - аппаратура разделения.

В общем случае групповой сигнал может формироваться не только простейшим суммированием канальных сигналов, но также и определенной логической обработкой, в результате которой каждый элемент группового сигнала несет информацию о сообщениях источников. Это так называемые системы с комбинационным разделением.

Чтобы разделяющие устройства были в состоянии различать сигналы отдельных каналов, должны существовать определенные признаки, присущие только данному сигналу. Такими признаками в общем случае могут быть параметры переносчика, например амплитуда, частота или фаза в случае непрерывной модуляции гармонического переносчика. При дискретных видах модуляции различающим признаком может служить и форма сигналов. Соответственно различаются и способы разделения сигналов: частотный, временной, фазовый и др.

Поскольку всякая реальная линия связи обладает ограниченной полосой пропускания, то при многоканальной передаче каждому отдельному каналу отводится определенная часть общей полосы пропускания.

На приемной стороне одновременно действуют сигналы всех каналов, различающиеся положением их частотных спектров на шкале частот. Чтобы без взаимных помех разделить такие сигналы, приемные устройства должны содержать частотные фильтры. Каждый из фильтров должен пропустить без ослабления лишь те частоты, которые принадлежат сигналу данного канала; частоты сигналов всех других каналов фильтр должен подавить.

Для снижения переходных помех до допустимого уровня приходится вводить защитные частотные интервалы (Рис. 11)

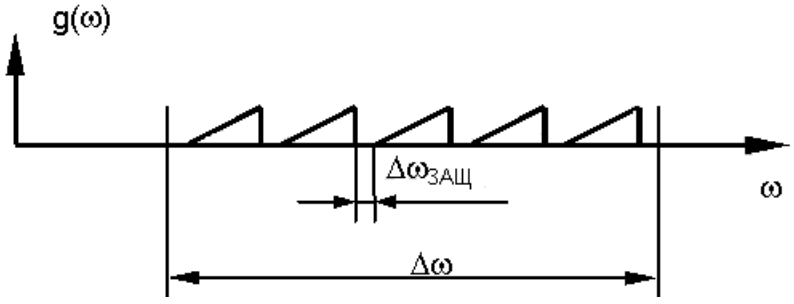


Рисунок 11. Спектр группового сигнала с защитными интервалами

При однократном преобразовании спектра сигнала (***fн = 104 кГц***) необходим специальный фильтр. При двукратном преобразовании спектра в первом модуляторе выбирается несущая до 30 кГц, например, ***f1 = 12 кГц***. При этом фильтр легко реализуется на ***LC***-элементах. На второй модулятор сигнал подается уже в полосе частот ***12,3…15,4 кГц***, и для переноса этого сигнала в заданную полосу частот необходимо использовать несущую ***f2 = 104 - f1 = 92 кГц***. Фильтр второго преобразователя частоты также легко реализуется на ***LC***-элементах.

Методы построения многоканальной аппаратуры с ЧРК отличаются способом формирования группового сигнала и особенностями передачи его в линейном тракте. По способу формирования группового сигнала (первый признак) различают:
1. метод с индивидуальным преобразованием сигналов;
2. метод с групповым преобразованием сигналов.
По способу усиления группового (линейного) сигнала (второй признак) выделяют:
1. метод с усилением каждого индивидуального сигнала;
2. метод с усилением линейного сигнала в целом.

При индивидуальном преобразовании сигналов формирование группового (линейного) спектра частот производится путем отдельного независимого преобразования каждого из ***N*** сигналов. Другими словами, при индивидуальном методе преобразователи, фильтры, усилители и другие элементы для каждого канала являются отдельными и повторяются в составе оконечной промежуточной аппаратуры столько раз, на сколько каналов рассчитана система передачи. Индивидуальные методы преобразования в оконечных и усиления в промежуточных станциях поясняются на рис. 12.

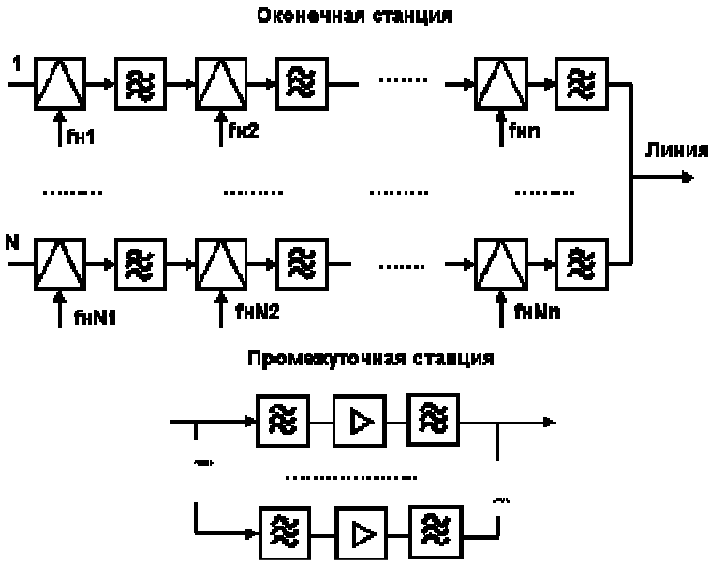


Рисунок 12. Индивидуальный метод преобразования

В основу метода группового преобразования сигналов положен принцип формирования линейного спектра в оконечном пункте МКС с помощью нескольких ступеней преобразования. На каждой ступени объединяются несколько канальных сигналов, т.е. линейный сигнал представляет собой сумму нескольких промежуточных групповых сигналов. При этом, в отличие от индивидуального метода, отдельной для каждого канала является только часть аппаратуры, а остальное оборудование – общее для всех каналов.

1.3 Лекция №3 (2 часа).

Тема: «Линии связи».

1.3.1 Вопросы лекции:

1. Спектральный анализ сигналов на линии связи.

2. Характеристики линии связи.

1.3.2 Краткое содержание вопросов:

1. Спектральный анализ сигналов на линии связи.

Из теории гармонического анализа известно, что любой периодический процесс можно представить в виде суммы синусоидальных колебаний различных частот и различных амплитуд (рис. 13). Каждая составляющая синусоида называется также гармоникой, а набор всех гармоник называют спектральным разложением исходного сигнала. Непериодические сигналы можно представить в виде интеграла синусоидальных сигналов с непрерывным спектром частот. Например, спектральное разложение

идеального импульса (единичной мощности и нулевой длительности) имеет составляющие всего спектра частот, от - ∞ до + ∞ (рис. 14).

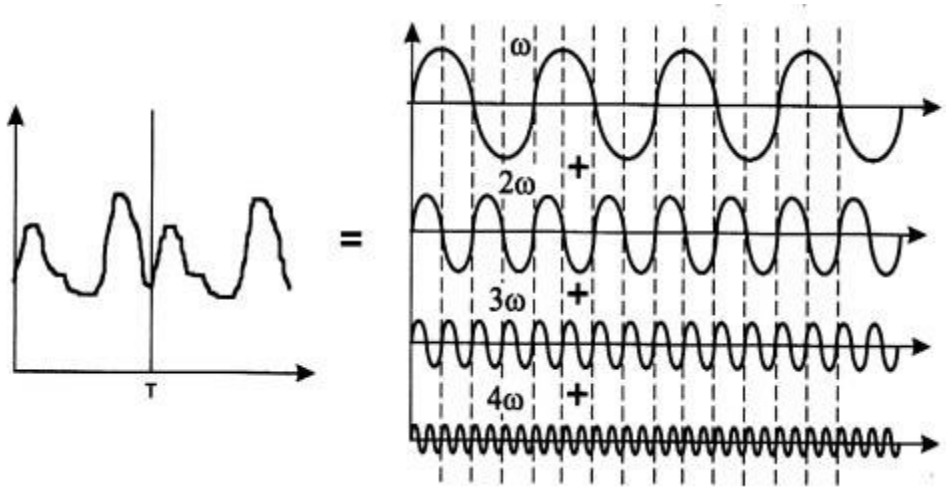


Рисунок 13. Представление периодического сигнала суммой синусоид

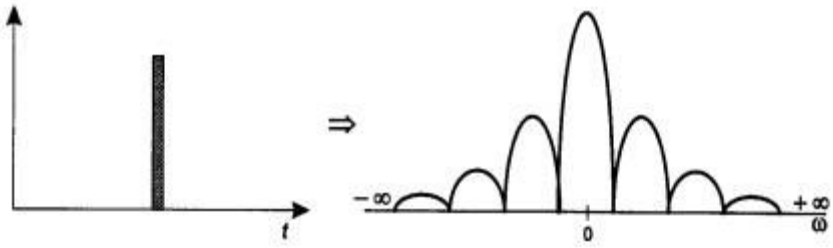


Рисунок 14. Спектральное разложение идеального импульса

Техника нахождения спектра любого исходного сигнала хорошо известна. Для некоторых сигналов, которые хорошо описываются аналитически (например, для последовательности прямоугольных импульсов одинаковой длительности и амплитуды), спектр легко вычисляется на основании формул Фурье. Для сигналов произвольной формы, встречающихся на практике, спектр можно найти с помощью специальных приборов - спектральных анализаторов, которые измеряют спектр реального сигнала и отображают амплитуды составляющих гармоник на экране или распечатывают их на принтере. Искажение передающим каналом синусоиды какой-либо частоты приводит в конечном счете к искажению передаваемого сигнала любой формы, особенно если синусоиды различных частот искажаются неодинаково. Если это аналоговый сигнал, передающий речь, то изменяется тембр голоса за счет искажения обертонов - боковых частот. При передаче импульсных сигналов, характерных для компьютерных сетей, искажаются низкочастотные и высокочастотные гармоники, в результате фронты

импульсов теряют свою прямоугольную форму. Вследствие этого на приемном конце линии сигналы могут плохо распознаваться.

Линия связи искажает передаваемые сигналы из-за того, что ее физические параметры отличаются от идеальных. Так, например, медные провода всегда представляют собой некоторую распределенную по длине комбинацию активного сопротивления, емкостной и индуктивной нагрузки . В результате для синусоид различных частот линия будет обладать различным полным сопротивлением, а значит, и передаваться они будут по-разному. Волоконно-оптический кабель также имеет отклонения, мешающие идеальному распространению света. Если линия связи включает промежуточную аппаратуру, то она также может вносить дополнительные искажения, так как невозможно создать устройства, которые бы одинаково хорошо передавали весь спектр синусоид, от нуля до бесконечности.

Кроме искажений сигналов, вносимых внутренними физическими параметрами линии связи, существуют и внешние помехи, которые вносят свой вклад в искажение формы сигналов на выходе линии. Эти помехи создают различные электрические двигатели, электронные устройства, атмосферные явления и т. д. Несмотря на защитные меры, предпринимаемые разработчиками кабелей и усилительно-коммутирующей аппаратуры, полностью компенсировать влияние внешних помех не удается. Поэтому сигналы на выходе линии связи обычно имеют сложную, по которой иногда трудно понять, какая дискретная информация была подана на вход линии

.

2. Характеристики линии связи.

К основным характеристикам линий связи относятся:

- амплитудно-частотная характеристика;
- полоса пропускания;
- затухание;
- помехоустойчивость;
- перекрестные наводки на ближнем конце линии;
- пропускная способность;
- достоверность передачи данных;
- удельная стоимость.

В первую очередь разработчика вычислительной сети интересуют пропускная способность и достоверность передачи данных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети. Пропускная способность и достоверность - это характеристики как линии связи, так и способа передачи данных.

Поэтому если способ передачи (протокол) уже определен, то известны и эти характеристики. Например, пропускная способность цифровой линии всегда известна, так как на ней определен протокол физического уровня, который задает битовую скорость передачи данных - 64 Кбит/с, 2 Мбит/с и т. п.

Однако нельзя говорить о пропускной способности линии связи, до того как для нее определен протокол физического уровня. Именно в таких случаях, когда только предстоит определить, какой из множества существующих протоколов можно использовать на данной линии, очень важными являются остальные характеристики линии, такие как полоса пропускания, перекрестные наводки, помехоустойчивость и другие характеристики.

Для определения характеристик линии связи часто используют анализ ее реакций на некоторые эталонные воздействия. Такой подход позволяет достаточно просто и однотипно определять характеристики линий связи любой природы, не прибегая к сложным теоретическим исследованиям. Чаще всего в качестве эталонных сигналов для исследования реакций линий связи используются синусоидальные сигналы различных частот. Это связано с тем, что сигналы этого типа часто встречаются в технике и с их помощью можно представить любую функцию времени - как непрерывный процесс колебаний звука, так и прямоугольные импульсы, генерируемые компьютером.

Амплитудно-частотная характеристика (рис. 15) показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала. Вместо амплитуды в этой характеристике часто используют также такой параметр сигнала, как его мощность.

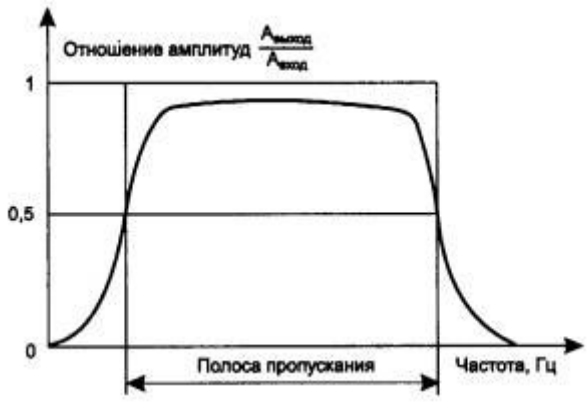


Рисунок 15. Амплитудно-частотная характеристика

Знание амплитудно-частотной характеристики реальной линии позволяет определить форму выходного сигнала практически для любого входного сигнала. Для

этого необходимо найти спектр входного сигнала, преобразовать амплитуду составляющих его гармоник в соответствии с амплитудно-частотной характеристикой, а затем найти форму выходного сигнала, сложив преобразованные гармоники.

Полоса пропускания (bandwidth) – это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала к входному превышает некоторый заранее заданный предел, обычно 0,5. То есть полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений. Знание полосы пропускания позволяет получить с некоторой степенью приближения тот же результат, что и знание амплитудно-частотной характеристики. Ширина полосы пропускания в наибольшей степени влияет на максимально возможную скорость передачи информации по линии связи. Именно этот факт нашел отражение в английском эквиваленте рассматриваемого термина (width - ширина).

Затухание (attenuation) определяется как относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты. Таким образом, затухание представляет собой одну точку из амплитудно-частотной характеристики линии. Часто при эксплуатации линии заранее известна основная частота передаваемого сигнала, то есть та частота, гармоника которой имеет наибольшую амплитуду и мощность. Поэтому достаточно знать затухание на этой частоте, чтобы приблизительно оценить искажения передаваемых по линии сигналов. Более точные оценки возможны при знании затухания на нескольких частотах, соответствующих нескольким основным гармоникам передаваемого сигнала.

Затухание А обычно измеряется в децибелах (дБ, decibel – dB) и вычисляется по следующей формуле:

$$A = 10 \log_{10} P_{вых} / P_{вх},$$

где $P_{вых}$ – мощность сигнала на выходе линии,

$P_{вх}$ – мощность сигнала на входе линии.

Так как мощность выходного сигнала кабеля без промежуточных усилителей всегда меньше, чем мощность входного сигнала, затухание кабеля всегда является отрицательной величиной.

Абсолютный уровень мощности, например, уровень мощности передатчика, также измеряется в децибелах. При этом в качестве базового значения мощности сигнала, относительно которого измеряется текущая мощность, принимается значение в 1 мВт (милливатт). Таким образом, уровень мощности р вычисляется по следующей формуле:

$$p = 10 \log_{10} P/1мВт \text{ [дБм]},$$

где Р - мощность сигнала в милливаттах

дБм (dBm) – это единица измерения уровня мощности (децибел на 1 мВт).

Пропускная способность (throughput) линии характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду – бит/с, а также в производных единицах, таких как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т. д.

Пропускная способность линий связи и коммуникационного сетевого оборудования традиционно измеряется в битах в секунду, а не в байтах в секунду.

Пропускная способность линии связи зависит не только от ее характеристик, таких как амплитудно-частотная характеристика, но и от спектра передаваемых сигналов. Если значимые гармоники сигнала (то есть те гармоники, амплитуды которых вносят основной вклад в результирующий сигнал) попадают в полосу пропускания линии, то такой сигнал будет хорошо передаваться данной линией связи и приемник сможет правильно распознать информацию, отправленную по линии передатчиком. Если же значимые гармоники выходят за границы полосы пропускания линии связи, то сигнал будет значительно искажаться, приемник будет ошибаться при распознавании информации, а значит, информация не сможет передаваться с заданной пропускной способностью.

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной – волоконно-оптические линии, малочувствительные ко внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

Перекрестные наводки на ближнем конце (Near End Cross Talk - NEXT) определяют помехоустойчивость кабеля к внутренним источникам помех, когда электромагнитное поле сигнала, передаваемого выходом передатчика по одной паре проводников, наводит на другую пару проводников сигнал помехи. Если ко второй паре будет подключен приемник, то он может принять наведенную внутреннюю помеху за полезный сигнал. Показатель NEXT, выраженный в децибелах, равен

10 log2 Рвых/Рнав,

где Рвых – мощность выходного сигнала,

Рнав – мощность наведенного сигнала.

Чем меньше значение NEXT, тем лучше кабель. Так, для витой пары категории 5 показатель NEXT должен быть меньше –27 дБ на частоте 100 МГц.

Показатель NEXT обычно используется применительно к кабелю, состоящему из нескольких витых пар, так как в этом случае взаимные наводки одной пары на другую могут достигать значительных величин. Для одинарного коаксиального кабеля (то есть состоящего из одной экранированной жилы) этот показатель не имеет смысла, а для двойного коаксиального кабеля он также не применяется вследствие высокой степени защищенности каждой жилы. Оптические волокна также не создают сколь-нибудь заметных помех друг для друга.

В связи с тем, что в некоторых новых технологиях используется передача данных одновременно по нескольким витым парам, в последнее время стал применяться показатель PowerSUM, являющийся модификацией показателя NEXT. Этот показатель отражает суммарную мощность перекрестных наводок от всех передающих пар в кабеле.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют интенсивностью битовых ошибок (Bit Error Rate, BER). Величина BER для каналов связи без дополнительных средств защиты от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило,10-4 – 10-6, в оптоволоконных линиях связи – 10-9. Значение достоверности передачи данных, например, в 10-4 говорит о том, что в среднем из 10000 бит искажается значение одного бита.

Искажения бит происходят как из-за наличия помех на линии, так и по причине искажений формы сигнала ограниченной полосой пропускания линии. Поэтому для повышения достоверности передаваемых данных нужно повышать степень помехозащищенности линии, снижать уровень перекрестных наводок в кабеле, а также использовать более широкополосные линии связи.

1.4 Лекция №4 (2 часа).

Тема: «Сетевые модели»

1.4.1 Вопросы:

1. Сетевая модель OSI.

2. Структура стандартов IEEE 802.X.

1.4.2 Краткое содержание вопросов:

1. Сетевая модель OSI.

Международная Организация по Стандартам (МОС, International Standards Organization – ISO) предложила в качестве стандарта открытых систем семиуровневую коммуникационную модель (рис.1.19), известную как OSI-модель (Open Systems Interconnection) – модель Взаимодействия Открытых Систем (ВОС).

Каждый уровень OSI-модели отвечает за отдельные специфические функции в коммуникациях и реализуется техническими и программными средствами вычислительной сети.

Физический уровень

Уровень 1 – физический (physical layer) – самый низкий уровень OSI-модели, определяющий процесс прохождения сигналов через среду передачи между сетевыми устройствами (узлами сети).

Реализует управление каналом связи:

- подключение и отключение канала связи;
- формирование передаваемых сигналов и т.п.

Описывает:

- механические, электрические и функциональные характеристики среды передачи;
- средства для установления, поддержания и разъединения физического соединения.

Обеспечивает при необходимости:

- кодирование данных;
- модуляцию сигнала, передаваемого по среде.

Данные физического уровня представляют собой поток битов (последовательность нулей или единиц), закодированные в виде электрических, оптических или радио сигналов.

Из-за наличия помех, воздействующих на электрическую линию связи, достоверность передачи, измеряемая как вероятность искажения одного бита, составляет 10-4 – 10 -6. Это означает, что в среднем на 10000 – 1000000 бит передаваемых данных один бит оказывается искажённым.

Канальный уровень

Канальный уровень или уровень передачи данных (data link layer) является вторым уровнем OSI-модели.

Реализует управление:

- доступом сетевых устройств к среде передачи, когда два или более устройств могут использовать одну и ту же среду передачи;
- надежной передачей данных в канале связи, позволяющей увеличить достоверность передачи данных на 2-4 порядка.

Описывает методы доступа сетевых устройств к среде передачи, основанные, например, на передаче маркера или на соперничестве.

Обеспечивает:

- функциональные и процедурные средства для установления, поддержания и разрыва соединения;
- управление потоком для предотвращения переполнения приемного устройства, если его скорость меньше, чем скорость передающего устройства;
- надежную передачу данных через физический канал с вероятностью искажения данных 10-8 – 10 -9 за счёт применения методов и

средства контроля передаваемых данных и повторной передачи данных при обнаружении ошибки.

Таким образом, канальный уровень обеспечивает достаточно надежную передачу данных через ненадежный физический канал.

Блок данных, передаваемый на канальном уровне, называется кадром (frame).

На канальном уровне появляется свойство адресуемости передаваемых данных в виде физических (машинных) адресов, называемых также MAC-адресами и являющихся обычно уникальными идентификаторами сетевых устройств.

Как будет показано в разделе 3, универсальные MAC-адреса в ЛВС Ethernet и Token Ring являются 6-байтными и записываются в шестнадцатеричном виде, причём байты адреса разделены дефисом, например: 00-19-45-A2-B4-DE .

К процедурам канального уровня относятся:

- добавление в кадры соответствующих адресов;
- контроль ошибок;
- повторная, при необходимости, передача кадров.

На канальном уровне работают ЛВС Ethernet, Token Ring и FDDI.

Сетевой уровень

Сетевой уровень (network layer), в отличие от двух предыдущих, отвечает за передачу данных в СПД и управляет маршрутизацией сообщений – передачей через несколько каналов связи по одной или нескольким сетям, что обычно требует включения в пакет сетевого адреса получателя.

Блок данных, передаваемый на сетевом уровне, называется пакетом

(packet).

Сетевой адрес – это специфический идентификатор для каждой промежуточной сети между источником и приемником информации.

Сетевой уровень реализует:

- обработку ошибок,
- мультиплексирование пакетов;
- управление потоками данных.

Самые известные протоколы этого уровня:

- X.25 в сетях с коммутацией пакетов;
- IP в сетях TCP/IP;
- IPX/SPX в сетях NetWare.

Кроме того, к сетевому уровню относятся протоколы построения маршрутных таблиц для маршрутизаторов: OSPF, RIP, ES-IS, IS-IS.

Транспортный уровень

Транспортный уровень (transport layer) наиболее интересен из высших уровней для администраторов и разработчиков сетей, так как он управляет сквозной передачей сообщений между оконечными узлами сети ("end-end"), обеспечивая надежность и экономическую эффективность передачи данных независимо от пользователя. При этом оконечные узлы возможно взаимодействуют через несколько узлов или даже через несколько транзитных сетей.

На транспортном уровне реализуется:

1) преобразование длинных сообщений в пакеты при их передаче в сети и обратное преобразование;
2) контроль последовательности прохождения пакетов;
3) регулирование трафика в сети;
4) распознавание дублированных пакетов и их уничтожение.

Способ коммуникации "end-end" облегчается еще одним способом адресации – адресом процесса, который соотносится с определенной прикладной программой (прикладным процессом), выполняемой на компьютере. Компьютер обычно выполняет одновременно несколько программ, в связи с чем необходимо знать какой прикладной программе (процессу) предназначено поступившее сообщение. Для этого на транспортном уровне используется специальный адрес, называемый адресом порта. Сетевой уровень доставляет каждый пакет на конкретный адрес компьютера, а транспортный уровень передаёт полностью собранное сообщение конкретному прикладному процессу на этом компьютере.

Транспортный уровень может предоставлять различные типы сервисов, в частности, передачу данных без установления соединения или с предварительным установлением соединения. В последнем случае перед началом передачи данных с использованием специальных управляющих пакетов устанавливается соединение с транспортным уровнем компьютера, которому предназначены передаваемые данные. После того как все данные переданы, подключение заканчивается. При передаче данных без установления соединения транспортный уровень используется для передачи одиночных пакетов, называемых дейтаграммами, не гарантируя их надежную доставку. Передача данных с установлением соединения применяется для надежной доставки данных.

Сеансовый уровень

Сеансовый уровень (session layer) обеспечивает обслуживание двух "связанных" на уровне представления данных объектов сети и управляет ведением диалога между ними путем синхронизации, заключающейся в установке служебных меток внутри длинных сообщений. Эти метки позволяют после обнаружения ошибки повторить передачу данных не с самого начала, а только с того места, где находится ближайшая предыдущая метка по отношению к месту возникновения ошибки.

Сеансовый уровень предоставляет услуги по организации и синхронизации обмена данными между процессами уровня представлений.

На сеансовом уровне реализуется:

1) установление соединения с адресатом и управление сеансом;
2) координация связи прикладных программ на двух рабочих станциях.

Уровень представления

Уровень представления (presentation layer) обеспечивает совокупность служебных операций, которые можно выбрать на прикладном уровне для интерпретации передаваемых и получаемых данных. Эти служебные операции включают в себя:

- управление информационным обменом;
- преобразование (перекодировка) данных во внутренний формат каждой конкретной ЭВМ и обратно;
- шифрование и дешифрование данных с целью защиты от несанкционированного доступа;
- сжатие данных, позволяющее уменьшить объём передаваемых данных, что особенно актуально при передаче мультимедийных данных, таких как аудио и видео.

Служебные операции этого уровня представляют собой основу всей семиуровневой модели и позволяют связывать воедино терминалы и средства вычислительной техники (компьютеры) самых разных типов и производителей.

Прикладной уровень

Прикладной уровень (application layer) обеспечивает непосредственную поддержку прикладных процессов и программ конечного пользователя, а также управление взаимодействием этих программ с различными объектами сети. Другими словами, прикладной уровень обеспечивает интерфейс между прикладным ПО и системой связи. Он предоставляет прикладной программе доступ к различным сетевым службам, включая передачу файлов и электронную почту.

2. Структура стандартов IEEE 802.X.

В 1980 году в институте IEEE был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов IEEE 802-x, которые содержат рекомендации по проектированию нижних уровней локальных сетей. Позже результаты работы этого комитета легли в основу комплекса международных стандартов ISO 8802-1...5. Эти стандарты были созданы на основе очень распространенных фирменных стандартов сетей Ethernet, ArcNet и Token Ring.

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

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

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

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

Уровень 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, то есть отличающихся качеством транспортных услуг этого уровня.

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

Стандарты IEEE 802 имеют достаточно четкую структуру, приведенную на рис. 16:

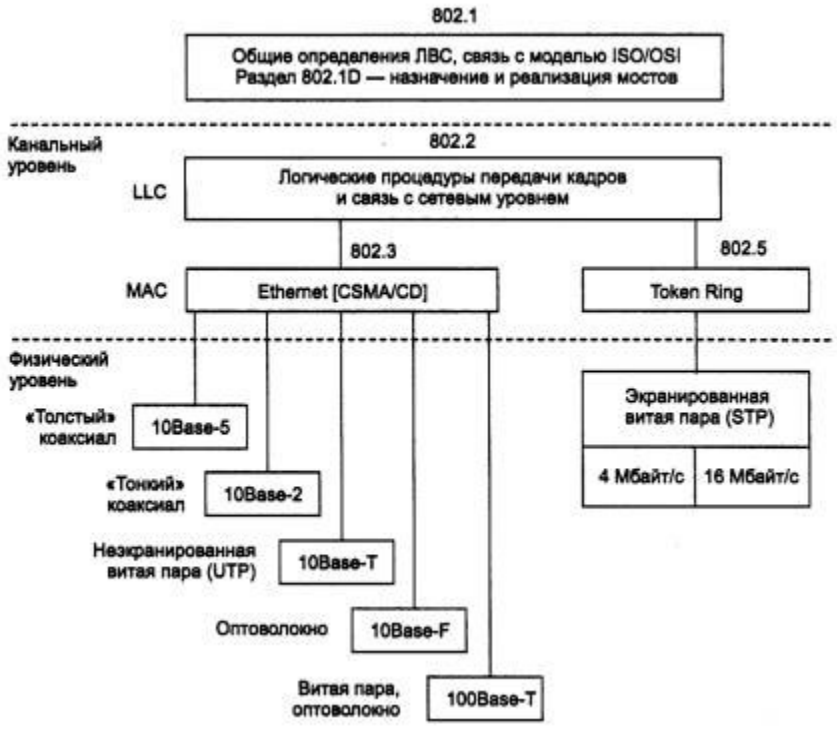


Рисунок 16. Структура стандартов IEEE 802.X

Эта структура появилась в результате большой работы, проведенной комитетом 802 по выделению в разных фирменных технологиях общих подходов и общих функций, а также согласованию стилей их описания. В результате канальный уровень был разделен на два упомянутых подуровня. Описание каждой технологии разделено на две части: описание уровня MAC и описание физического уровня. Как видно из рисунка, практически у каждой технологии единственному протоколу уровня MAC соответствует несколько вариантов протоколов физического уровня (на рисунке в целях экономии места приведены только технологии Ethernet и Token Ring, но все сказанное справедливо также и для остальных технологий, таких как ArcNet, FDDI, l00VG-AnyLAN).

Над канальным уровнем всех технологий изображен общий для них протокол LLC, поддерживающий несколько режимов работы, но независимый от выбора конкретной технологии. Стандарт LLC курирует подкомитет 802.2. Даже технологии, стандартизованные не в рамках комитета 802, ориентируются на использование протокола LLC, определенного стандартом 802.2, например протокол FDDI, стандартизованный ANSI.

Особняком стоят стандарты, разрабатываемые подкомитетом 802.1. Эти стандарты носят общий для всех технологий характер. В подкомитете 802.1 были разработаны общие определения локальных сетей и их свойств, определена связь трех уровней модели IEEE 802 с моделью OSI. Но наиболее практически важными являются стандарты 802.1, которые описывают взаимодействие между собой различных технологий, а также стандарты по построению более сложных сетей на основе базовых топологий. Эта группа стандартов носит общее название стандартов межсетевого взаимодействия (internetworking). Сюда входят такие важные стандарты, как стандарт 802. ID, описывающий логику работы моста/коммутатора, стандарт 802.1H, определяющий работу транслирующего моста, который может без маршрутизатора объединять сети Ethernet и FDDI, Ethernet и Token Ring и т. п. Сегодня набор стандартов, разработанных подкомитетом 802.1, продолжает расти. Например, недавно он пополнился важным стандартом 802.1Q, определяющим способ построения виртуальных локальных сетей VLAN в сетях на основе коммутаторов.

Стандарты 802.3,802.4,802.5 и 802.12 описывают технологии локальных сетей, которые появились в результате улучшений фирменных технологий, легших в их основу. Так, основу стандарта 802.3 составила технология Ethernet, разработанная компаниями Digital, Intel и Xerox (или Ethernet DIX), стандарт 802.4 появился | как обобщение

технологии ArcNet компании Datapoint Corporation, а стандарт 802.5 в основном соответствует технологии Token Ring компании IBM.

Исходные фирменные технологии и их модифицированные варианты - стандарты 802.x в ряде случаев долгие годы существовали параллельно. Например, технология ArcNet так до конца не была приведена в соответствие со стандартом 802.4 (теперь это делать поздно, так как где-то примерно с 1993 года производство оборудования ArcNet было свернуто). Расхождения между технологией Token Ring и стандартом 802.5 тоже периодически возникают, так как компания IBM регулярно вносит усовершенствования в свою технологию и комитет 802.5 отражает эти усовершенствования в стандарте с некоторым запозданием. Исключение составляет технология Ethernet. Последний фирменный стандарт Ethernet DIX был принят в 1980 году, и с тех пор никто больше не предпринимал попыток фирменного развития Ethernet. Все новшества в семействе технологий Ethernet вносятся только в результате принятия открытых стандартов комитетом 802.3.

Более поздние стандарты изначально разрабатывались не одной компанией, а группой заинтересованных компаний, а потом передавались в соответствующий подкомитет IEEE 802 для утверждения. Так произошло с технологиями Fast Ethernet, l00VG-AnyLAN, Gigabit Ethernet. Группа заинтересованных компаний образовывала сначала небольшое объединение, а затем по мере развития работ к нему присоединялись другие компании, так что процесс принятия стандарта носил открытый характер.

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

802.1 - Internetworking - объединение сетей;

802.2 - Logical Link Control, LLC - управление логической передачей данных;

802.3 - Ethernet с методом доступа CSMA/CD;

802.4 - Token Bus LAN - локальные сети с методом доступа Token Bus;

802.5 - Token Ring LAN - локальные сети с методом доступа Token Ring;

802.6 - Metropolitan Area Network, MAN - сетимегаполисов;

802.7 - Broadband Technical Advisory Group - техническая консультационная группа по широкополосной передаче;

802,8 - Fiber Optic Technical Advisory Group - техническая консультационная группа по волоконно-оптическим сетям;

802.9 - Integrated Voice and data Networks - интегрированные сети передачи голоса и данных;

802.10 - Network Security - сетевая безопасность;

802.11 - Wireless Networks - беспроводные сети;

802.12 - Demand Priority Access LAN, l00VG-AnyLAN - локальные сети с методом доступа по требованию с приоритетами.

1.5 Лекция №5 (2 часа).

Тема: «Сетевое оборудование»

1.5.1 Вопросы лекции:

1. Сетевые адаптеры.
2. Концентраторы.
3. Коммутаторы.
4. Маршрутизатор.

1.5.2 Краткое содержание вопросов:

1. Сетевые адаптеры.

Сетевой адаптер (Network Interface Card, NIC) - это периферийное устройство компьютера, непосредственно взаимодействующее со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации. Сетевые адаптеры и кабели являются аппаратной основой организации компьютерных сетей, их нормальная работа жизненно важна для сети. С кабелями и адаптерами связано обычно 80% неполадок в сети.

Сетевой адаптер вместе со своим драйвером реализует второй, канальный уровень модели открытых систем в конечном узле сети – компьютере.

Сетевой адаптер совместно с драйвером выполняет две операции: передачу и прием кадра.

В каждом компьютере должен быть установлен сетевой адаптер, обеспечивающий подключение к выбранному типу кабеля. Платы сетевого адаптера выступают в качестве физического интерфейса, или соединения между компьютером и сетевым кабелем. Платы вставляются в слоты расширения всех сетевых компьютеров и серверов.

В большинстве современных стандартов для локальных сетей предполагается, что между сетевыми адаптерами взаимодействующих компьютеров устанавливается специальное коммуникационное устройство (концентратор, мост, коммутатор или

маршрутизатор), которое берет на себя некоторые функции по управлению потоком данных.

Сетевой адаптер обычно выполняет следующие функции:

• Формирование передаваемой информации в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.

• Получение доступа к среде передачи данных. В локальных сетях в основном применяются разделяемые между группой компьютеров каналы связи (общая шина, кольцо), доступ к которым предоставляется по специальному алгоритму (наиболее часто применяются метод случайного доступа или метод с передачей маркера доступа по кольцу).

• Кодирование последовательности бит кадра последовательностью электрических сигналов при передаче данных и декодирование при их приеме.

• Преобразование информации из параллельной формы в последовательную и обратно. Эта операция связана с тем, что для упрощения проблемы синхронизации сигналов и удешевления линий связи в вычислительных сетях информация передается в последовательной форме, бит за битом, а не побайтно, как внутри компьютера.

• Синхронизация битов, байтов и кадров. Для устойчивого приема передаваемой информации необходимо поддержание постоянного синхронизма приемника и передатчика информации. Сетевой адаптер использует для решения этой задачи специальные методы кодирования, не использующие дополнительной шины с тактовыми синхросигналами. Эти методы обеспечивают периодическое изменение состояния передаваемого сигнала, которое используется тактовым генератором приемника для подстройки синхронизма. Кроме синхронизации на уровне битов, сетевой адаптер решает задачу синхронизации и на уровне байтов, и на уровне кадров.

Функцией сетевого адаптера является передача и прием сетевых сигналов из кабеля. Адаптер воспринимает команды и данные от сетевой операционной системы (ОС), преобразует эту информацию в один из стандартных форматов и передает ее в сеть через подключенный к адаптеру кабель.

Сетевые адаптеры различаются также по типу принятой в сети сетевой технологии - Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую

пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

2. Концентраторы.

Концентратор (hub) – это сетевое устройство, предназначенное для объединения устройств сети в сегменты. Основной принцип его работы заключается в трансляции пакетов, поступающих на один из его портов на все другие порты. Таким образом, пакет, поступивший в сеть, будет отправлен всем остальным устройствам сети, т.е. будет осуществляться широковещательная передача. Концентратор работает на физическом уровне модели взаимодействия открытых систем (OSI). Концентратор используется в различных технологиях: ATM, xDSL, Token Ring, но наибольшее распространение он нашел в технологии Ethernet.

Концентратор можно рассматривать как репитер с несколькими выходами. В отличие от switch он не анализирует содержимое пакетов или их заголовки, а просто копирует их. Hub не позволяет увеличить число устройств в одном сегменте или разгрузить его, уменьшив число коллизий. Основная его задача – это подключение новых устройств к сети и организация ее топологии. Кроме того, hub может быть использован для организации резервных каналов.

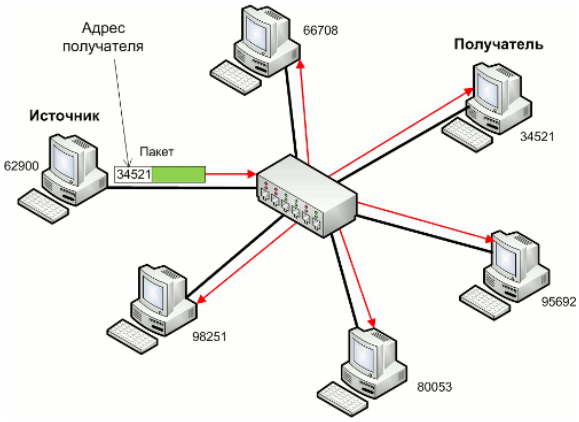


Рисунок 17. Пример работы сети с концентратором

Главным достоинством концентратора является простота реализации и, соответственно, невысокая стоимость. Однако из-за того, что он просто копирует пакеты во все свои порты, то в сети увеличивается вероятность возникновения коллизий. Это может привести к снижению скорости передачи и времени доставки пакетов. Именно поэтому вместо концентраторов обычно стараются применять коммутаторы, которые передают пакеты только к тому порту, к которому подключен компьютер получатель.

В зависимости от выполняемых задач можно встретить различные по емкости концентраторы от 4 до 64 портов. Однако это не предел. Они могут объединяться в более емкие устройства. Максимально возможное число работающих в спаренном режиме устройств ограничивается лишь характеристиками используемой технологии (для Ethernet – 1024 портов в одном сегменте). Концентраторы отличаются также по типу используемых проводников (витая пара, коаксиальный кабель) и используемой среде передачи (электрический или оптический кабель).

3. Коммутаторы.

Сетевой коммутатор (network switch) – это устройство, используемое в сетях передачи пакетов, предназначенное для объединения нескольких сегментов. В отличие от маршрутизатора (router) коммутатор работает на канальном уровне модели OSI, что и определяет главные различия между ними. Коммутатор не занимается расчетом маршрута для дальнейшей передачи пакетов по сети, анализируя различные факторы, как это делает маршрутизатор. Switch только передает данные от одного порта к другому на основе содержащейся в пакете информации. Обычно признаком выбора выходного порта служит MAC-адрес устройства, к которому передаются данные. В свою очередь коммутатор в отличие от концентратора или репитера не просто транслирует порты ко всем выходам, которые у него есть, а к одному, заранее выбранному.

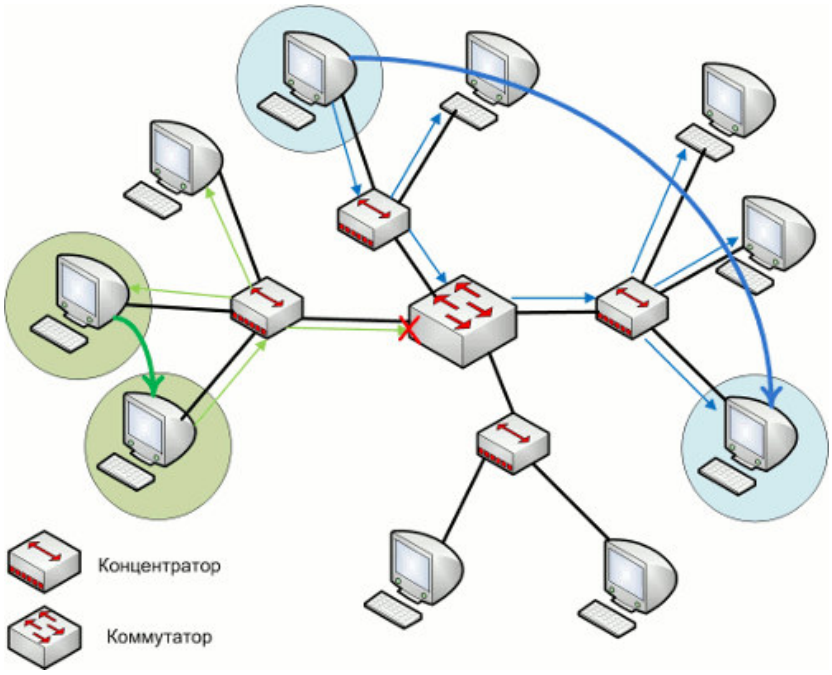


Рисунок 18. Пример сети с коммутатором

Сетевые коммутаторы применяются в нескольких технологиях, но наибольшее распространение нашли в Ethernet. Главной их задачей в сети Ethernet является разделение сети на сегменты. Это особенно актуально в сетях с большим числом рабочих станций, т.к. чем больше оконечных устройств работают одновременно с единой средой передачи данных тем выше вероятность возникновения коллизии (одновременной передачи данных несколькими устройствами) и, следовательно, ниже эффективность работы сети. Коммутатор позволяет разбить единую сеть на несколько сегментов и увеличить число одновременно работающих устройств.

Существую управляемые и неуправляемые коммутаторы. Неуправляемые коммутаторы самонастраиваются после включения в сеть. Они анализируют MAC-адреса всех устройств, подключенных к ним и будут осуществлять коммутацию между портами на основе анализа заголовка пакета, в котором содержится MAC-адресом устройства-получателя. Управляемые коммутаторы предоставляют интерфейс для администратора, который может выполнить его настройку для работы в конкретной сети. Например, есть возможность выбора режима защиты от отказа (в случае работы в паре с резервным коммутатором), объединения нескольких портов в единое направление, настройки приоритетов и резервирования портов и мн. др. Обычно управляемые коммутаторы дороже и используются в емких сетях, с дополнительными требованиями по надежности.

Switch может быть выполнен и в виде небольшой платы на 4 порта и многополочного штатива с возможность интеграции дополнительных устройств и расширения емкости. Также в зависимости от назначения сетевой коммутатор может снабжаться автономным питанием, портами управления и резервирования, охлаждением.

4. Маршрутизатор.

Маршрутизатор – это устройство пакетной сети передачи данных, предназначенное для объединения сегментов сети и ее элементов и служит для передачи пакетов между ними на основе каких-либо правил. Маршрутизаторы работают на сетевом (третьем) уровне модели OSI в качестве узловых устройств для различных технологий: IP, ATM, Frame Relay и мн. др.

Одной из самых важных задач маршрутизаторов является выбор оптимального маршрута передачи пакетов между подключенными сетями. Причем сделать это необходимо максимально оперативно с минимальной временной задержкой. Одновременно с этим должна отслеживаться текущая обстановка в сети для исключения из возможных путей доставки перегруженные и поврежденные участки. Практически все маршрутизаторы используют в своей работе, так называемые, таблицы маршрутизации. Это своеобразные базы данных, которые содержат информацию обо всех возможных

маршрутах передачи пакетов с некоторой дополнительной информацией, которая берется в расчет при выборе оптимального варианта доставки. Это может быть состояние канала, время доставки информации, загруженность, полоса пропускания и др.

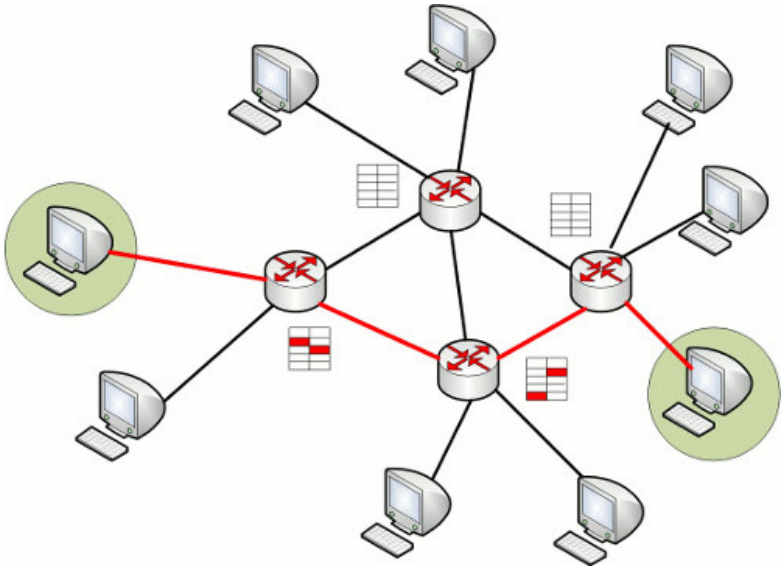


Рисунок 19. Пример работы маршрутизаторов в сети пакетной передачи данных

Важным аспектом работы маршрутизаторов является способ обновления информации в таблицах маршрутизации. Это может выполняться двумя способами вручную и автоматически. В первом случае администратор сети самостоятельно настраивает таблицы маршрутизации. Такой вариант подходит только для небольших сетей, конфигурация которых изменяется редко. Маршрутизаторы первого типа называются статическими. Автоматическое обновление таблиц маршрутизации выполняется с помощью обмена информационными сообщениями между соседними маршрутизаторами о текущей обстановке, а также проверке соединительных каналов между ними.Такие маршрутизаторы называются динамическими. Главный их недостаток заключается в необходимости дополнительных сетевых и вычислительных ресурсов для обмена данными и расчета маршрута. Однако динамические маршрутизаторы могут быть использованы при построении сетей любого масштаба.

Маршрутизаторы бывают как проводные – наиболее классический тип с несколькими портами, в которые подключаются кабели от внешних устройств, так и беспроводные, например, используемые для построения сетей WiFi. Также маршрутизаторы значительно различаются по емкости. Это могут быть как небольшие роутеры с 8-12 портами, которые используются при построении локальных сетей, так и громоздкие модульные конструкции, рассчитанные на сотни подключаемых сегментов.

1.6 Лекция №6 (2 часа).

Тема: «Протоколы маршрутизации»

1.6.1 Вопросы:

1. Классификация протоколов маршрутизации.

2. Алгоритмы маршрутизации.

3. Внешние и внутренние шлюзовые протоколы.

1.6.2 Краткое содержание вопросов:

1.Классификация протоколов маршрутизации

Протоколы маршрутизации предназначены для автоматического построения таблиц маршрутизации, на основе которых происходит продвижение пакетов сетевого уровня. Протоколы маршрутизации, в отличие от сетевых протоколов, таких как IP и IPX, не являются обязательными, так как таблица маршрутизации может быть построена администратором сети вручную. При этом в крупных сетях со сложной топологией и большим количеством альтернативных маршрутов протоколы маршрутизации выполняют очень важную и полезную работу, автоматизируя построение таблиц маршрутизации, динамически адаптируя текущий набор рабочих маршрутов к состоянию сети и повышая тем самым ее производительность и надежность.

В настоящее время существует ряд протоколов обеспечивающих маршрутизацию в Ad-Hoc сетях. По принципу поиска маршрута выделяют три класса протоколов: проактивные, реактивные и комбинированные.

Проактивные протоколы маршрутизации

Эти типы протоколов обеспечивают предварительное построение таблице маршрутизации, в которую включаются все известные маршруты. Подобный подход используют все протоколы маршрутизации в проводных локальных сетях. В этом случае, пересылка пакетов начинается без задержек, но присутствуют накладные расходы на поиск маршрутов и построение таблице маршрутизации, потому что необходимо получить всю необходимую информацию о топологии сети до начала передачи пакетов. В дальнейшем данные протоколы предполагают дополнительные расходы на поддержание маршрутной информации в актуальном виде. Примерамиявляются DSDV (Destination Sequenced Distance Vector), OLSR (Optimized Link State Routing).

Реактивные протоколы маршрутизации

Эти типы протоколов называются протоколами по требованию. Узлы не хранят необходимую маршрутную информацию все время. Узел инициирует построение маршрута по требованию, в момент поступления запроса на передачу данных. Этот

механизм построения маршрута основан на алгоритме наводнения, узел просто передает первый пакет всем своим соседям, а промежуточные узлы перенаправляют его далее, к своим соседям. Это повторяющиеся действия позволяют доставить пакет до пункта назначения. Как правило, при прохождении пакета запоминается маршрут прохождения (например, в виде списка задействованных узлов) и впоследствии при передаче последующих пакетов эта информация используются для выбора направления. Реактивные методы имеют меньшие накладные расходы на маршрутизацию, но большую задержку при инициации передачи, потому что маршрут между узлами будет найден только тогда, когда один из узлов получит запрос на передачу. Примеромреактивныхпротоколовявляются DSR(Dynamic Source Routing), AODV(Ad hoc On-Demand Distance Vector), TOPA(Temporally ordered routing algorithm).

Гибридные протоколы маршрутизации

Гибридные протоколы являются комбинации реактивного и проактивного подходов. Они используют преимущества этих двух протоколов и, как следствие, достаточно эффективно работают в отдельных случаях. Примером гибридного протокола может являться ZRP (Zone Routing Protocol) и HWMP (Hybrid Wireless Mesh Protocol).

2. Алгоритмы маршрутизации.

Алгоритмы маршрутизации применяются для определения оптимального пути пакетов от источника к получателю и являются основой любого протокола маршрутизации.

Типы алгоритмов

Алгоритмы маршрутизации могут быть классифицированы по типам:

•Статические или динамические. Статические алгоритмы представляют свод правил работы со статическими таблицами маршрутизации, которые настраиваются администраторами сети. Хорошо работают в случае предсказуемого трафика в сетях стабильной конфигурации. Динамические алгоритмы маршрутизации подстраиваются к изменяющимся обстоятельствам сети в масштабе реального времени. Они выполняют это путем анализа поступающих сообщений об обновлении маршрутизации. Если в сообщении указывается, что имело место изменение сети, программы маршрутизации пересчитывают маршруты и рассылают новые сообщения о корректировке маршрутизации. Такие сообщения пронизывают сеть, стимулируя маршрутизаторы заново прогонять свои алгоритмы и соответствующим образом изменять таблицы маршрутизации. Динамические алгоритмы маршрутизации могут дополнять, где это уместно, статические маршруты.

•Одномаршрутные или многомаршрутные алгоритмы. Некоторые сложные протоколы маршрутизации обеспечивают множество маршрутов к одному и тому же пункту назначения. Такие многомаршрутные алгоритмы делают возможной мультиплексную передачу трафика по многочисленным линиям, одномаршрутные алгоритмы не могут делать этого. Многомаршрутные алгоритмы могут обеспечить значительно большую пропускную способность и надежность.

•Одноуровневые или иерархические алгоритмы. Отличаются по принципу взаимодействия друг с другом. В одноуровневой системе маршрутизации все рутеры равны по отношению друг к другу. В иерархической системе маршрутизации пакеты данных перемещаются от роутеров нижнего уровня к базовым, которые осуществляют основную маршрутизацию. Как только пакеты достигают общей области пункта назначения, ониперемежаются вниз по иерархии до хоста назначения.

•Алгоритмы с маршрутизацией от источника. В системах маршрутизации от источника роутеры действуют просто как устройства хранения и пересылки пакета, безвсякий раздумий отсылая его к следующей остановке, они предполагают, что отправитель рассчитывает и определяет весь маршрут сам. Другие алгоритмы предполагают, что хост отправителя ничего не знает о маршрутах. При использовании такого рода алгоритмов роутеры определяют маршрут через сеть, базируясь на своих собственных расчетах.

•Внутридоменные или междоменные алгоритмы. Некоторые алгоритмы маршрутизации действуют только в пределах доменов; другие - как в пределах доменов, так и между ними.

•Алгоритмы состояния канала и дистанционно-векторные. Алгоритмы состояния канала направляют потоки маршрутной информации во все узлы сети. Каждый роутер отсылает только ту часть известной ему информации, которая описывает состояние его собственных каналов, но всем узлам маршрутизации. Дистанционно-векторные требуют от каждого роутера пересылки всей или части его таблицы но только соседям.

Качество алгоритма определяется следующими показателями:

- Оптимальность,
- Простота и низкие непроизводительные затраты,
- Живучесть и стабильность,
- Быстрая сходимость,
- Гибкость.

Оптимальность

Оптимальность характеризует способность алгоритма маршрутизации выбирать "наилучший" маршрут. Наилучший маршрут зависит от показателей и от "веса" этих показателей, используемых при проведении расчета.

Простота и низкие непроизводительные затраты

Алгоритмы маршрутизации разрабатываются как можно более простыми, чтобы эффективно обеспечивать свои функциональные возможности, с мимимальными затратами программного обеспечения. Особенно это важно, когда маршрутизация, должна выполняться в компьютере с ограниченными физическими ресурсами.

Живучесть и стабильность

Алгоритмы маршрутизации должны обладать живучестью. Другими словами, они должны четко функционировать в случае неординарных или непредвиденных обстоятельств, таких как отказы аппаратуры, условия высокой нагрузки и некорректные реализации. Т.к. роутеры расположены в узловых точках сети, их отказ может вызвать значительные проблемы.

Часто наилучшими алгоритмами маршрутизации оказываются те, которые выдержали испытание временем и доказали свою надежность в различных условиях работы сети.

Быстрая сходимость

Алгоритмы маршрутизации должны быстро сходиться. Сходимость - это процесс соглашения между всеми роутерами по оптимальным маршрутам. Когда какое-нибудь событие в сети приводит к тому, что маршруты или отвергаются, или наоборот, становятся доступными, роутеры рассылают сообщения об обновлении маршрутизации. Такие сообщения пронизывают сети, стимулируя пересчет оптимальных маршрутов и, в конечном итоге, вынуждая все роутеры придти к соглашению по этим маршрутам. Алгоритмы маршрутизации, которые сходятся медленно, могут привести к образованию петель маршрутизации или выходам из строя сети.

Гибкость

Алгоритмы маршрутизации должны быть также гибкими, т.е. быстро и точно адаптироваться к разнообразным обстоятельствам в сети, таким как изменения полосы пропускания сети, размеров очереди к роутеру, величины задержки сети и других переменных. Например, предположим, что сегмент сети отвергнут. Многие алгоритмы

маршрутизации, после того как они узнают об этой проблеме, быстро выбирают следующий наилучший путь для всех маршрутов, которые обычно используют этот сегмент.

Маршрутные таблицы содержат информацию, которую используют программы для выбора наилучшего маршрута. Ниже перечислены показатели, которые используются в алгоритмах маршрутизации:

- Длина маршрута,
- Надежность,
- Задержка,
- Ширина полосы пропускания,
- Нагрузка,
- Стоимость связи.

Сложные алгоритмы маршрутизации при выборе маршрута могут базироваться на множестве показателей, комбинируя их таким образом, что в результате получается один отдельный (гибридный) показатель.

Длина маршрута

Длина маршрута является наиболее общим показателем маршрутизации. Некоторые протоколы маршрутизации позволяют администраторам сети назначать произвольные цены на каждый канал сети. В этом случае длиной тракта является сумма расходов, связанных с каждым каналом. Другие протоколы маршрутизации определяют "количество пересылок", т.е. показатель, характеризующий число проходов, которые пакет должен совершить на пути от источника до пункта назначения через изделия об'единения сетей (такие как роутеры).

Надежность

Надежность каждого канала сети в контексте алгоритмов маршрутизации обычно описывается в терминах отношения бит/ошибка. Некоторые каналы сети могут отказывать чаще, чем другие. Отказы одних каналов сети могут быть устранены легче или быстрее, чем отказы других каналов. При назначении оценок надежности могут быть приняты в расчет любые факторы надежности. Оценки надежности обычно назначаются каналам сети администраторами сети. Как правило, это произвольные цифровые величины.

Задержка

Под задержкой маршрутизации обычно понимают отрезок времени, необходимый для передвижения пакета от источника до пункта назначения через об'единенную сеть. Задержка зависит от многих факторов, включая полосу пропускания промежуточных каналов сети, очереди в порт каждого роутера на пути передвижения пакета, перегруженность сети на всех промежуточных каналах сети и физическое расстояние, на которое необходимо переместить пакет. Т.к. здесь имеет место конгломерация нескольких важных переменных, задержка является наиболее общим и полезным показателем.

Полоса пропускания

Полоса пропускания относится к имеющейся мощности трафика какого-либо канала. При прочих равных показателях, канал Ethernet 10 Mbps предпочтителен любой арендованной линии с полосой пропускания 64 Кбайт/сек. Хотя полоса пропускания является оценкой максимально достижимой пропускной способности канала, маршруты, проходящие через каналы с большей полосой пропускания, не обязательно будут лучше маршрутов, проходящих через менее быстродействующие каналы.

3. Внешние и внутренние шлюзовые протоколы.

Такое решение было найдено для самой крупной на сегодня составной сети — Интернета. Это решение базируется на понятии автономной системы.

Обычно автономной системой управляет один поставщик услуг Интернета, самостоятельно выбирая, какие протоколы маршрутизации должны использоваться в некоторой автономной системе и каким образом между ними должно выполняться перераспределение маршрутной информации. Крупные поставщики услуг и корпорации могут представить свою составную сеть как набор нескольких автономных систем. Регистрация автономных систем происходит централизованно, как и регистрация IP-адресов и DNS-имен. Номер автономной системы состоит из 16 разрядов и никак не связан с префиксами IP-адресов входящих в нее сетей.

В соответствии с этой концепцией Интернет выглядит как набор взаимосвязанных автономных систем, каждая из которых состоит из взаимосвязанных сетей (рис. 20), соединенными внешними шлюзами.

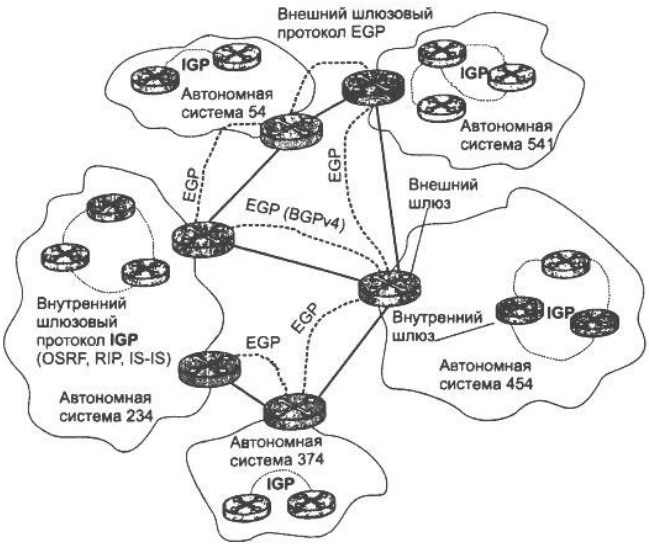


Рисунок 20 Автономные системы Интернета

Основная цель деления Интернета на автономные системы — обеспечение многоуровневого подхода к маршрутизации. До введения автономных систем предполагался двухуровневый подход, то есть сначала маршрут определялся как последовательность сетей, а затем вел непосредственно к заданному узлу в конечной сети (именно этот подход мы использовали до сих пор).

С появлением автономных систем появляется третий, верхний, уровень маршрутизации — теперь сначала маршрут определяется как последовательность автономных систем, затем — как последовательность сетей и только потом ведет к конечному узлу.

Выбор маршрута между автономными системами осуществляют внешние шлюзы, использующие особый тип протокола маршрутизации, так называемый внешний шлюзовой протокол (Exterior Gateway Protocol, EGP). В настоящее время для работы в такой роли сообщество Интернета утвердило стандартный пограничный шлюзовой протокол версии 4 (Border Gateway Protocol, BGPv4). В качестве адреса следующего маршрутизатора в протоколе BGPv4 указывается адрес точки входа в соседнюю автономную систему.

За маршрут внутри автономной системы отвечают внутренние шлюзовые протоколы (Interior Gateway Protocol, IGP). К числу IGP относятся знакомые нам протоколы RIP, OSPF и IS-IS. В случае транзитной автономной системы эти протоколы указывают точную последовательность маршрутизаторов от точки входа в автономную систему до точки выхода из нее.

Внутри каждой автономной системы может применяться любой из существующих протоколов маршрутизации, в то время как между автономными системами всегда применяется один и тот же протокол, являющийся своеобразным языком «эсперанто», на котором автономные системы общаются между собой.

Концепция автономных систем скрывает от администраторов магистрали Интернета проблемы маршрутизации пакетов на более низком уровне — уровне сетей. Для администратора магистрали неважно, какие протоколы маршрутизации применяются внутри автономных систем, для него существует единственный протокол маршрутизации — BGPv4.

1.7 Лекция №7,8 (4 часа).

Тема: «Протокол TCP/IP»

1.7.1 Вопросы:

1. Протоколы TCP/IP.

2. Архитектура TCP/IP.

1.7.2 Краткое содержание вопросов:

1. Протоколы TCP/IP.

TCP/IP - это два основных сетевых протокола Internet. Часто это название используют и для обозначения сетей, работающих на их основе. Протокол IP (Internet Protocol - IP v4) обеспечивает маршрутизацию (доставку по адресу) сетевых пакетов. Протокол TCP (Transfer Control Protocol) обеспечивает установление надежного соединения между двумя машинами и собственно передачу данных, контролируя оптимальный размер пакета передаваемых данных и осуществляя перепосылку в случае сбоя. Число одновременно устанавливаемых соединений между абонентами сети не ограничивается, т. е. любая машина может в некоторый промежуток времени обмениваться данными с любым количеством других машин по одной физической линии.

Другое важное преимущество сети с протоколами TCP/IP состоит в том, что по нему могут быть объединены машины с разной архитектурой и разными операционными системами, например Unix, VAX VMS, MacOS, MS-DOS, MS Windows и т.д. Причем машины одной системы при помощи сетевой файловой системы NFS (Net File System) могут подключать к себе диски с файловой системой совсем другой ОС и оперировать "чужими" файлами как своими.

Протоколы TCP/IP (Transmission Control Protocol/Internet Protocol) являются базовыми транспортным и сетевым протоколами в OS UNIX. В заголовке TCP/IP пакета указывается:

IP-адрес отправителяIP-адрес получателяНомер порта (Фактически - номер прикладной программы, которой этот пакет предназначен)

Пакеты TCP/IP имеют уникальную особенность добраться до адресата, пройдя сквозь разнородные в том числе и локальные сети, используя разнообразные физические носители.Маршрутизацию IP-пакета (переброску его в требуемую сеть) осуществляют на добровольных началах компьютеры, входящие в TCP/IP сеть.

Протокол IP - это протокол, описывающий формат пакета данных, передаваемого по сети.

Следующий простой пример можетн прояснить, каким образом происходит передача данных и передача данных. Когда Вы получаете телеграмму, весь текст в ней (и адрес, и сообщение) написан на ленте подряд, но есть правила, позволяющие понять, где тут адрес, а где сообщение. Аналогично, пакет в компьютерной сети представляет собой поток битов, а протокол IP определяет, где адрес и прочая служебная информация, а где сами передаваемые данные. Таким образом, протокол IP в эталонной модели ISO/OSI является протоколомсетевого (3) уровня.

Протокол TCP - это протокол следующего уровня, предназначеный для контроля передачи и целостности передаваемой информации.

Когда Вы не расслышали, что сказал Вам собеседник в телефонном разговоре, Вы просите его повторить сказанное. Приблизительно этим занимается и протокол TCP применительно к компьютерным сетям. Компьютеры обмениваются пакетами протокола IP, контролируют их передачу по протоколу TCP и, объединяясь в глобальную сеть, образуют Интернет. Протокол TCP является протоколом транспортного (4) уровня.

2. Архитектура TCP/IP.

После того как семейство протоколов TCP/IP было реализовано и внедрено, Международная организация по стандартизации (International Organization for Standardization, ISO) предложила собственную семиуровневую сетевую модель, названную OSI (Open System Interconnection — взаимодействие открытых систем). Она так никогда и не приобрела широкой популярности из-за своей сложности и неэффективности.

В данной модели обмен информацией может быть представлен в виде стека, представленного на рисунке 21. Как видно из рисунка, в этой модели определяется все - от стандарта физического соединения сетей до протоколов обмена прикладного программного обеспечения. Дадим некоторые комментарии к этой модели.

Физический уровень данной модели определяет характеристики физической сети передачи данных, которая используется для межсетевого обмена. Это такие параметры, как: напряжение в сети, сила тока, число контактов на разъемах и т.п. Типичными стандартами этого уровня являются, например RS232C, V35, IEEE 802.3 и т.п.

Рисунок 21. Семиуровневая модель протоколов межсетевого обмена OSI

К канальному уровню отнесены протоколы, определяющие соединение, например, SLIP (Strial Line Internet Protocol), PPP (Point to Point Protocol), NDIS, пакетный протокол, ODI и т.п. В данном случае речь идет о протоколе взаимодействия между драйверами устройств и устройствами, с одной стороны, а с другой стороны, между операционной системой и драйверами устройства. Такое определение основывается на том, что драйвер - это, фактически, конвертор данных из оного формата в другой, но при этом он может иметь и свой внутренний формат данных.

К сетевому (межсетевому) уровню относятся протоколы, которые отвечают за отправку и получение данных, или, другими словами, за соединение отправителя и получателя. Вообще говоря, эта терминология пошла от сетей коммутации каналов, когда отправитель и получатель действительно соединяются на время работы каналом связи. Применительно к сетям TCP/IP, такая терминология не очень приемлема. К этому уровню в TCP/IP относят протокол IP (Internet Protocol). Именно здесь определяется отправитель и получатель, именно здесь находится необходимая информация для доставки пакета по сети.

Транспортный уровень отвечает за надежность доставки данных, и здесь, проверяя контрольные суммы, принимается решение о сборке сообщения в одно целое. В Internet транспортный уровень представлен двумя протоколами TCP (Transport Control Protocol) и UDP (User Datagramm Protocol). Если предыдущий уровень (сетевой) определяет только правила доставки информации, то транспортный уровень отвечает за целостность доставляемых данных.

Уровень сессии определяет стандарты взаимодействия между собой прикладного программного обеспечения. Это может быть некоторый промежуточный стандарт данных или правила обработки информации. Условно к этому уровню можно отнеси механизм портов протоколов TCP и UDP и Berkeley Sockets. Однако обычно, рамках архитектуры TCP/IP такого подразделения не делают.

Уровень обмена данными с прикладными программами (Presentation Layer) необходим для преобразования данных из промежуточного формата сессии в формат данных приложения. В Internet это преобразование возложено на прикладные программы.

Уровень прикладных программ или приложений определяет протоколы обмена данными этих прикладных программ. В Internet к этому уровню могут быть отнесены такие протоколы, как: FTP, TELNET, HTTP, GOPHER и т.п.

Вообще говоря, стек протоколов TCP отличается от только что рассмотренного стека модели OSI. Обычно его можно представить в виде схемы, представленной на рисунке 22.

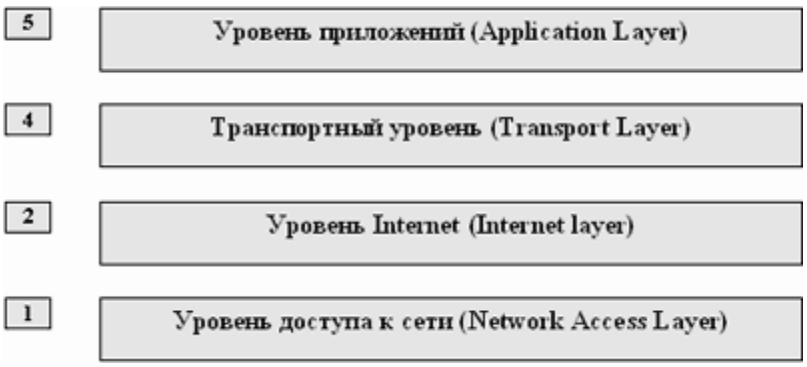


Рисунок 22. Структура стека протоколов TCP/IP

В этой схеме на уровне доступа к сети располагаются все протоколы доступа к физическим устройствам. Выше располагаются протоколы межсетевого обмена IP, ARP, ICMP. Еще выше основные транспортные протоколы TCP и UDP, которые кроме сбора пакетов в сообщения еще и определяют какому приложению необходимо данные отправить или от какого приложения необходимо данные принять. Над транспортным

уровнем располагаются протоколы прикладного уровня, которые используются приложениями для обмена данными.

Базируясь на классификации OSI (Open System Integration) всю архитектуру протоколов семейства TCP/IP попробуем сопоставить с эталонной моделью (рисунок 23).

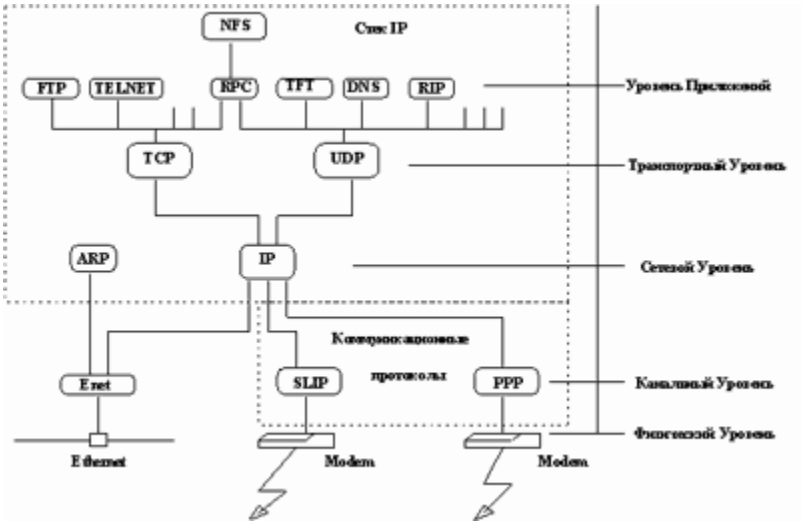


Рисунок 23. Схема модулей, реализующих протоколы семейства TCP/IP в узле сети

Прямоугольниками на схеме обозначены модули, обрабатывающие пакеты, линиями - пути передачи данных. Прежде чем обсуждать эту схему, введем необходимую для этого терминологию.

Драйвер - программа, непосредственно взаимодействующая с сетевым адаптером.

Модуль - это программа, взаимодействующая с драйвером, с сетевыми прикладными программами или с другими модулями.

Схема приведена для случая подключения узла сети через локальную сеть Ethernet, поэтому названия блоков данных будут отражать эту специфику.

Сетевой интерфейс - физическое устройство, подключающее компьютер к сети. В нашем случае - карта Ethernet.

Кадр - это блок данных, который принимает/отправляет сетевой интерфейс.

IP-пакет - это блок данных, которым обменивается модуль IP с сетевым интерфейсом.

UDP-датаграмма - блок данных, которым обменивается модуль IP с модулем UDP.

TCP-сегмент - блок данных, которым обменивается модуль IP с модулем TCP.

Прикладное сообщение - блок данных, которым обмениваются программы сетевых приложений с протоколами транспортного уровня.

Инкапсуляция - способ упаковки данных в формате одного протокола в формат другого протокола. Например, упаковка IP-пакета в кадр Ethernet или TCP-сегмента в IP-пакет. Согласно словарю иностранных слов термин "инкапсуляция" означает "образование капсулы вокруг чужих для организма веществ (инородных тел, паразитов и т.д.)". В рамках межсетевого обмена понятие инкапсуляции имеет несколько более расширенный смысл. Если в случае инкапсуляции IP в Ethernet речь идет действительно о помещении пакета IP в качестве данных Ethernet-фрейма, или, в случае инкапсуляции TCP в IP, помещение TCP-сегмента в качестве данных в IP-пакет, то при передаче данных по коммутируемым каналам происходит дальнейшая "нарезка" пакетов теперь уже на пакеты SLIP или фреймы PPP.

Рисунок 24. Инкапсуляция протоколов верхнего уровня в протоколы TCP/IP

Вся схема (рисунок 24) называется стеком протоколов TCP/IP или просто стеком TCP/IP. Чтобы не возвращаться к названиям протоколов расшифруем аббревиатуры TCP, UDP, ARP, SLIP, PPP, FTP, TELNET, RPC, TFTP, DNS, RIP, NFS:

TCP - Transmission Control Protocol - базовый транспортный протокол, давший название всему семейству протоколов TCP/IP.

UDP - User Datagram Protocol - второй транспортный протокол семейства TCP/IP. Различия между TCP и UDP будут обсуждены позже.

ARP - Address Resolution Protocol - протокол используется для определения соответствия IP-адресов и Ethernet-адресов.

SLIP - Serial Line Internet Protocol (Протокол передачи данных по телефонным линиям).

PPP - Point to Point Protocol (Протокол обмена данными "точка-точка").

FTP - File Transfer Protocol (Протоколобменафайлами).

TELNET - протокол эмуляции виртуального терминала.

RPC - Remote Process Control (Протокол управления удаленными процессами).

TFTP - Trivial File Transfer Protocol (Тривиальный протокол передачи файлов).

DNS - Domain Name System (Системадоменныхимен).

RIP - Routing Information Protocol (Протоколмаршрутизации).

NFS - Network File System (Распределенная файловая система и система сетевой печати).

При работе с такими программами прикладного уровня, как FTP или telnet, образуется стек протоколов с использованием модуля TCP, представленный на рисунке 25.

Рисунок 25. Стек протоколов при использовании модуля TCP

При работе с прикладными программами, использующими транспортный протокол UDP, например, программные средства Network File System (NFS), используется другой стек, где вместо модуля TCP будет использоваться модуль UDP (рисунок 26).

Рисунок 26. Стек протоколов при работе через транспортный протокол UDP

При обслуживании блочных потоков данных модули TCP, UDP и драйвер ENET работают как мультиплексоры, т.е. перенаправляют данные с одного входа на несколько выходов и наоборот, с многих входов на один выход. Так, драйвер ENET может направить кадр либо модулю IP, либо модулю ARP, в зависимости от значения поля "тип" в заголовке кадра. Модуль IP может направить IP-пакет либо модулю TCP, либо модулю UDP, что определяется полем "протокол" в заголовке пакета.

Получатель UDP-датаграммы или TCP-сообщения определяется на основании значения поля "порт" в заголовке датаграммы или сообщения.

Все указанные выше значения прописываются в заголовке сообщения модулями на отправляющем компьютере. Так как схема протоколов - это дерево, то к его корню ведет только один путь, при прохождении которого каждый модуль добавляет свои данные в заголовок блока. Машина, принявшая пакет, осуществляет демультиплексирование в соответствии с этими отметками.

Технология Internet поддерживает разные физические среды, из которых самой распространенной является Ethernet. В последнее время большой интерес вызывает подключение отдельных машин к сети через TCP-стек по коммутируемым (телефонным) каналам. С появлением новых магистральных технологий типа ATM или FrameRelay активно ведутся исследования по инкапсуляции TCP/IP в эти протоколы. На сегодняшний день многие проблемы решены и существует оборудование для организации TCP/IP сетей через эти системы.

1.8 Лекция №9 (2 часа).

Тема: «Кодирование информации»

1.8.1 Вопросы:

1. Выборка способа кодирования.

2. Методы кодирования.

1.8.2 Краткое содержание вопросов:

1. Выборка способа кодирования.

Код — это набор условных обозначений (или сигналов) для записи (или передачи) некоторых заранее определенных понятий.

Кодирование информации – это процесс формирования определенного представления информации. В более узком смысле под термином «кодирование» часто понимают переход от одной формы представления информации к другой, более удобной для хранения, передачи или обработки.

Обычно каждый образ при кодировании (иногда говорят — шифровке) представлен отдельным знаком.

Знак - это элемент конечного множества отличных друг от друга элементов.

В более узком смысле под термином "кодирование" часто понимают переход от одной формы представления информации к другой, более удобной для хранения, передачи или обработки.

Компьютер может обрабатывать только информацию, представленную в числовой форме. Вся другая информация (например, звуки, изображения, показания приборов и т. д.) для обработки на компьютере должна быть преобразована в числовую форму. Например, чтобы перевести в числовую форму музыкальный звук, можно через небольшие промежутки времени измерять интенсивность звука на определенных частотах, представляя результаты каждого измерения в числовой форме. С помощью программ для компьютера можно выполнить преобразования полученной информации, например "наложить" друг на друга звуки от разных источников.

Аналогичным образом на компьютере можно обрабатывать текстовую информацию. При вводе в компьютер каждая буква кодируется определенным числом, а при выводе на внешние устройства (экран или печать) для восприятия человеком по этим числам строятся изображения букв. Эти изображения называются литерами букв. Соответствие между набором букв и числами называется кодировкой символов.

Как правило, все числа в компьютере представляются с помощью нулей и единиц (а не десяти цифр, как это привычно для людей). Иными словами, компьютеры обычно работают в двоичной системе счисления, поскольку при этом устройства для их обработки получаются значительно более простыми. Ввод чисел в компьютер и вывод их для чтения человеком может осуществляться в привычной десятичной форме, а все необходимые преобразования выполняют программы, работающие на компьютере.

Одна и та же информация может быть представлена (закодирована) в нескольких формах. С появлением компьютеров возникла необходимость кодирования всех видов информации, с которыми имеет дело и отдельный человек, и человечество в целом. Но решать задачу кодирования информации человечество начало задолго до появления компьютеров. Грандиозные достижения человечества - письменность и арифметика - есть не что иное, как система кодирования речи и числовой информации. Информация никогда не появляется в чистом виде, она всегда как-то представлена, как-то закодирована.

Двоичное кодирование – один из распространенных способов представления информации. В вычислительных машинах, в роботах и станках с числовым программным управлением, как правило, вся информация, с которой имеет дело устройство, кодируется в виде слов двоичного алфавита только двумя знаками 0 и 1 (то есть все информация в памяти компьютера хранится и обрабатывается в виде последовательности нулей и единиц).

Кодирование символьной (текстовой) информации.

Основная операция, производимая над отдельными символами текста - сравнение символов.

При сравнении символов наиболее важными аспектами являются уникальность кода для каждого символа и длина этого кода, а сам выбор принципа кодирования практически не имеет значения.

Для кодирования текстов используются различные таблицы перекодировки. Важно, чтобы при кодировании и декодировании одного и того же текста использовалась одна и та же таблица.

Таблица перекодировки - таблица, содержащая упорядоченный некоторым образом перечень кодируемых символов, в соответствии с которой происходит преобразование символа в его двоичный код и обратно.

Наиболее популярные таблицы перекодировки: ДКОИ-8, ASCII, CP1251, Unicode.

Исторически сложилось, что в качестве длины кода для кодирования символов было выбрано 8 знаков. Любой из знаков 0 или 1 несет в себе 1 бит информации, следовательно один любой символ хранимый в памяти компьютера имеет информационный объем 8 бит (1 байт).

Различных комбинаций из 0 и 1 при длине кода 8 бит может быть 28 = 256, поэтому с помощью одной таблицы перекодировки можно закодировать не более 256 символов. При длине кода в 2 байта (16 бит) можно закодировать 65536 символов.

2. Методы кодирования.

В сетях применяются так называемые самосинхронизирующиеся коды, сигналы которых несут для передатчика указания о том, в какой момент времени нужно осуществлять распознавание очередного бита (или нескольких битов, если код ориентирован более чем на два состояния сигнала). Любой резкий перепад сигнала — так называемый фронт — может служить хорошим указанием для синхронизации приемника с передатчиком.

При использовании синусоид в качестве несущего сигнала результирующий код обладает свойством самосинхронизации, так как изменение амплитуды несущей частоты дает возможность приемнику определить момент появления входного кода.

Распознавание и коррекцию искаженных данных сложно осуществить средствами физического уровня, поэтому чаще всего эту работу берут на себя протоколы, лежащие выше: канальный, сетевой, транспортный или прикладной. С другой стороны, распознавание ошибок на физическом уровне экономит время, так как приемник не ждет полного помещения кадра в буфер, а отбраковывает его сразу при распознавании ошибочных битов внутри кадра.

Требования, предъявляемые к методам кодирования, являются взаимно противоречивыми, поэтому каждый из рассматриваемых ниже популярных методов цифрового кодирования обладает своими преимуществами и своими недостатками по сравнению с другими.

Потенциальный код без возвращения к нулю отражает то обстоятельство, что при передаче последовательности единиц сигнал не возвращается к нулю в течение такта (как мы увидим ниже, в других методах кодирования возврат к нулю в этом случае происходит). Метод NRZ прост в реализации, обладает хорошей распознаваемостью ошибок (из-за двух резко отличающихся потенциалов), но не обладает свойством самосинхронизации. При передаче длинной последовательности единиц или нулей сигнал на линии не изменяется, поэтому приемник лишен возможности определять по входному сигналу моменты времени, когда нужно в очередной раз считывать данные. Даже при наличии высокоточного тактового генератора приемник может ошибиться с моментом съема данных, так как частоты двух генераторов никогда не бывают полностью идентичными. Поэтому при высоких скоростях обмена данными и длинных последовательностях единиц или нулей небольшое рассогласование тактовых частот может привести к ошибке в целый такт и, соответственно, считыванию некорректного значения бита.

Другим серьезным недостатком метода NRZ является наличие низкочастотной составляющей, которая приближается к нулю при передаче длинных последовательностей единиц или нулей. Из-за этого многие каналы связи, не обеспечивающие прямого гальванического соединения между приемником и источником, этот вид кодирования не поддерживают. В результате в чистом виде код NRZ в сетях не используется. Тем не менее используются его различные модификации, в которых устраняют как плохую самосинхронизацию кода NRZ, так и проблемы постоянной составляющей. Привлекательность кода NRZ, из-за которой имеет смысл заняться его улучшением, состоит в достаточно низкой частоте основной гармоники /о, которая равна N/2 Гц, как это было показано в предыдущем разделе. У других методов кодирования, например манчестерского, основная гармоника имеет более высокую частоту.

Одной из модификаций метода NRZ является метод биполярного кодирования с альтернативной инверсией (Bipolar Alternate Mark Inversion, AMI). В этом методе (рис. 2.16, б) используются три уровня потенциала - отрицательный, нулевой и положительный. Для кодирования логического нуля используется нулевой потенциал, а логическая единица кодируется либо положительным потенциалом, либо отрицательным, при этом потенциал каждой новой единицы противоположен потенциалу предыдущей.

Код AMI частично ликвидирует проблемы постоянной составляющей и отсутствия самосинхронизации, присущие коду NRZ. Это происходит при передаче длинных последовательностей единиц. В этих случаях сигнал на линии представляет собой последовательность разнополярных импульсов с тем же спектром, что и у кода NRZ, передающего чередующиеся нули и единицы, то есть без постоянной составляющей и с основной гармоникой N/2 Гц (где N - битовая скорость передачи данных). Длинные же последовательности нулей также опасны для кода AMI, как и для кода NRZ - сигнал вырождается в постоянный потенциал нулевой амплитуды. Поэтому код AMI требует дальнейшего улучшения, хотя задача упрощается - осталось справиться только с последовательностями нулей.

В целом, для различных комбинаций бит на линии использование кода AMI приводит к более узкому спектру сигнала, чем для кода NRZ, а значит, и к более высокой пропускной способности линии. Например, при передаче чередующихся единиц и нулей основная гармоника fo имеет частоту N/4 Гц. Код AMI предоставляет также некоторые возможности по распознаванию ошибочных сигналов. Так, нарушение строгого чередования полярности сигналов говорит о ложном импульсе или исчезновении с линии корректного импульса. Сигнал с некорректной полярностью называется запрещенным сигналом (signal violation).

В коде AMI используются не два, а три уровня сигнала на линии. Дополнительный уровень требует увеличение мощности передатчика примерно на 3 дБ для обеспечения той же достоверности приема бит на линии, что является общим недостатком кодов с несколькими состояниями сигнала по сравнению с кодами, которые различают только два состояния.

Потенциальный код с инверсией при единице

Существует код, похожий на AMI, но только с двумя уровнями сигнала. При передаче нуля он передает потенциал, который был установлен в предыдущем такте (то есть не меняет его), а при передаче единицы потенциал инвертируется на противоположный. Этот код называется потенциальным кодом с инверсией при единице (Non Return to Zero with ones Inverted, NRZI). Этот код удобен в тех случаях, когда использование третьего уровня сигнала весьма нежелательно, например в оптических кабелях, где устойчиво распознаются два состояния сигнала - свет и темнота.

Для улучшения потенциальных кодов, подобных AMI и NRZI, используются два метода. Первый метод основан на добавлении в исходный код избыточных бит, содержащих логические единицы. Очевидно, что в этом случае длинные последовательности нулей прерываются и код становится самосинхронизирующимся для

любых передаваемых данных. Исчезает также постоянная составляющая, а значит, еще более сужается спектр сигнала. Но этот метод снижает полезную пропускную способность линии, так как избыточные единицы пользовательской информации не несут. Другой метод основан на предварительном «перемешивании» исходной информации таким образом, чтобы вероятность появления единиц и нулей на линии становилась близкой. Устройства, или блоки, выполняющие такую операцию, называются трамблерами (scramble - свалка, беспорядочная сборка). При скремб-лировании используется известный алгоритм, поэтому приемник, получив двоичные данные, передает их на дескрэмблер, который восстанавливает исходную последовательность бит. Избыточные биты при этом по линии не передаются. Оба метода относятся к логическому, а не физическому кодированию, так как форму сигналов на линии они не определяют. Более детально они изучаются в следующем разделе.

Биполярный импульсный код

Кроме потенциальных кодов в сетях используются и импульсные коды, когда данные представлены полным импульсом или же его частью - фронтом. Наиболее простым случаем такого подхода является биполярный импульсный код, в котором единица представлена импульсом одной полярности, а ноль - другой. Каждый импульс длится половину такта. Такой код обладает отличными самосинхронизирующими свойствами, но постоянная составляющая, может присутствовать, например, при передаче длинной последовательности единиц или нулей. Кроме того, спектр у него шире, чем у потенциальных кодов. Так, при передаче всех нулей или единиц частота основной гармоники кода будет равна N Гц, что в два раза выше основной гармоники кода NRZ и в четыре раза выше основной гармоники кода AMI при передаче чередующихся единиц и нулей. Из-за слишком широкого спектра биполярный импульсный код используется редко.

Манчестерский код

В локальных сетях до недавнего времени самым распространенным методом кодирования был так называемый манчестерский код. Он применяется в технологиях Ethernet и Token Ring.

В манчестерском коде для кодирования единиц и нулей используется перепад потенциала, то есть фронт импульса. При манчестерском кодировании каждый такт делится на две части. Информация кодируется перепадами потенциала, происходящими в середине каждого такта. Единица кодируется перепадом от низкого уровня сигнала к высокому, а ноль - обратным перепадом. В начале каждого такта может происходить служебный перепад сигнала, если нужно представить несколько единиц или нулей

подряд. Так как сигнал изменяется по крайней мере один раз за такт передачи одного бита данных, то манчестерский код обладает хорошими самосинхронизирующими свойствами. Полоса пропускания манчестерского кода уже, чем у биполярного импульсного. У него также нет постоянной составляющей, а основная гармоника в худшем случае (при передаче последовательности единиц или нулей) имеет частоту N Гц, а в лучшем (при передаче чередующихся единиц и нулей) она равна N/2 Гц, как и у кодов AMI или NRZ. В среднем ширина полосы манчестерского кода в полтора раза уже, чем у биполярного импульсного кода, а основная гармоника колеблется вблизи значения 3N/4. Манчестерский код имеет еще одно преимущество перед биполярным импульсным кодом. В последнем для передачи данных используются три уровня сигнала, а в манчестерском - два.

Потенциальный код 2B1Q

Потенциальный код с четырьмя уровнями сигнала для кодирования данных. Это код 2B1Q, название которого отражает его суть - каждые два бита (2B) передаются за один такт сигналом, имеющим четыре состояния (1Q), Паре бит 00 соответствует потенциал -2,5 В, паре бит 01 соответствует потенциал -0,833 В, паре 11 - потенциал +0,833 В, а паре 10 - потенциал +2,5 В. При этом способе кодирования требуются дополнительные меры по борьбе с длинными последовательностями одинаковых пар бит, так как при этом сигнал превращается в постоянную составляющую. При случайном чередовании бит спектр сигнала в два раза уже, чем у кода NRZ, так как при той же битовой скорости длительность такта увеличивается в два раза. Таким образом, с помощью кода 2B1Q можно по одной и той же линии передавать данные в два раза быстрее, чем с помощью кода AMI или NRZI. Однако для его реализации мощность передатчика должна быть выше, чтобы четыре уровня четко различались приемником на фоне помех.

1.9 Лекция №10 (2 часа).

Тема: «Метод CSMA/CB»

1.9.1 Вопросы лекции:

1. MAC адреса.
2. Доступ к среде и передача данных.
3. Возникновение коллизии.

1.9.2 Краткое содержание вопросов:

1. MAC адреса.

В сетях Ethernet используется метод доступа к среде передачи данных, называемый *методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD)*.

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

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

MAC-адрес (мак адрес) - это уникальный идентификатор сетевого интерфейса (обычно сетевой карты) для реализации коммуникации устройств в сети на физическом уровне.

Так, это уникальный номер, который хранится в доступной только для чтения памяти, назначенный сетевой карте ее производителем.

Стандарты IEEE определяют 48-разрядный (6 октетов) MAC-адрес, который разделен на четыре части.

Первые 3 октета (в порядке их передачи по сети; старшие 3 октета, если рассматривать их в традиционной бит-реверсной шестнадцатеричной записи MAC-адресов) содержат 24-битный уникальный идентификатор организации (OUI), или (Код MFG — Manufacturing, производителя), который производитель получает вIEEE. При этом используются только младшие 22 разряда (бита), 2 старшие имеют специальное назначение:

- первый бит (младший бит первого байта) указывает, для одиночного (0) или группового (1) адресата предназначен кадр
- второй младший бит первого байта указывает, является ли MAC-адрес глобально (0) или локально (1) администрируемым.

Следующие три октета выбираются изготовителем для каждого экземпляра устройства. За исключением сетей системной сетевой архитектуры SNA.

Таким образом, **глобально администрируемый MAC-адрес** устройства **глобально уникален** и обычно «зашит» в аппаратуру.

Администратор сети имеет возможность, вместо использования «зашитого», назначить устройству MAC-адрес по своему усмотрению. Такой **локально администрируемый MAC-адрес** выбирается произвольно и может не содержать информации об OUI. Признаком локально администрируемого адреса является соответствующий бит первого октета адреса (см. выше).

Для того, чтобы узнать MAC-адрес сетевого устройства, используются следующие команды:

- Windows — ipconfig /all — более подробно расписывает — какой MAC-адрес к какому сетевому интерфейсу относится
- Windows — getmac — менее подробно расписывает — какой MAC-адрес к какому сетевому интерфейсу относится
- Linux — ifconfig -a | grep HWaddr
- FreeBSD — ifconfig|grep ether
- HP-UX — /usr/sbin/lanscan
- Mac OS X — ifconfig, либо в Системных Настройках > Сеть > *выбрать подключение* > Дополнительно > Ethernet > Идентификатор Ethernet
- QNX4 — netinfo -l
- QNX6 — ifconfig или nicinfo

В общем, MAC-адрес назначается на постоянной основе устройству и не может быть изменен. Но в некоторых случаях существует возможность изменения MAC-адреса на программном уровне. Это известно, как MAC-спуфинг.

2. Доступ к среде и передача данных.

Предполагая для простоты изложения, что каждый узел (станция) имеет только один сетевой интерфейс, рассмотрим, как на основе алгоритма CSMA/CD происходит передача данных в сети Ethernet.

Все компьютеры в сети с разделяемой средой имеют возможность немедленно (с учетом задержки распространения сигнала по физической среде) получить данные, которые любой из компьютеров начал передавать в общую среду. Говорят, что среда, к которой подключены все станции, работает в режиме коллективного доступа (Multiply Access, MA).

Чтобы получить возможность передавать кадр, интерфейс-отправитель должен убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется несущей частотой (Carrier Sense, CS).

Признаком «незанятости» среды является отсутствие на ней несущей частоты, которая при манчестерском способе кодирования, принятом для всех вариантов Ethernet10 Мбит/с, равна 5-10 МГц в зависимости от последовательности единиц и нулей, передаваемых в данный момент.

Если среда свободна, то узел имеет право начать передачу кадра. В примере, показанном на рис. 27, узел 1 обнаружил, что среда свободна, и начал передавать свой кадр. В классической сети Ethernet на коаксиальном кабеле сигналы передатчика узла 1 распространяются в обе стороны, так что их получают все узлы сети. 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, идущих подряд, говорит приемнику о том, что преамбула закончилась и следующий бит является началом кадра.

Все станции, подключенные к кабелю, начинают записывать байты передаваемого кадра в свои внутренние буферы. Первые 6 байт кадра содержат адрес назначения. Та станция, которая узнает собственный адрес в заголовке кадра, продолжает записывать его содержимое в свой внутренний буфер, а остальные станции на этом прием кадра прекращают. Станция назначения обрабатывает полученные данные, передает их вверх по своему стеку. Кадр Ethernet содержит не только адрес назначения, но и адрес источника данных, поэтому станция-получатель знает, кому нужно послать ответ.

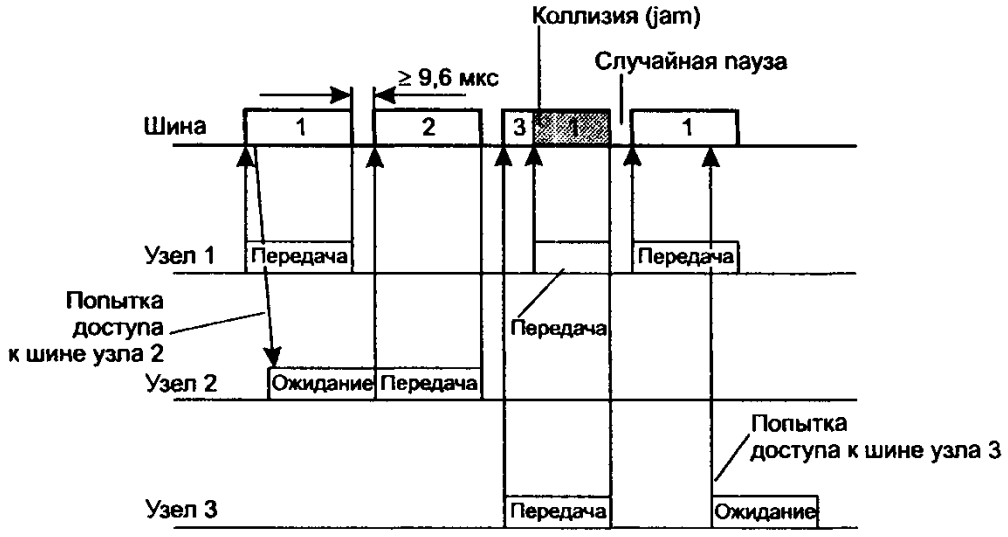


Рисунок 27 – Метод случайного доступа CSMA/CD

Узел 2 во время передачи кадра узлом 1 также пытался начать передачу своего кадра, однако обнаруживает, что среда занята – на ней присутствует несущая частота, – поэтому узел 2 вынужден ждать, пока узел 1 не прекратит передачу кадра.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу, равную межпакетному интервалу (Inter Packet Gap, IPG) в 9,6 мкс. Эта пауза нужна для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна. В приведенном примере узел 2 дождался окончания передачи кадра узлом 1, сделал паузу в 9,6 мкс и начал передачу своего кадра.

3. Возникновение коллизии.

Механизм прослушивания среды и пауза между кадрами не гарантируют исключения ситуации, когда две или более станции одновременно решают, что среда свободна, и начинают передавать свои кадры. Говорят, что при этом происходит коллизия, так как содержимое обоих кадров сталкивается на общем кабеле и происходит искажение информации.

Коллизия — это нормальная ситуация в работе сетей Ethernet. Для возникновения коллизии не обязательно, чтобы несколько станций начали передачу абсолютно одновременно, такая ситуация маловероятна. Более вероятна ситуация, когда один узел начинает передачу, а через некоторое (короткое) время другой узел, проверив среду и не обнаружив несущую (сигналы первого узла еще не успели до него дойти), начинает передачу своего кадра. Таким образом, возникновение коллизии является следствием распределения узлов сети в пространстве.

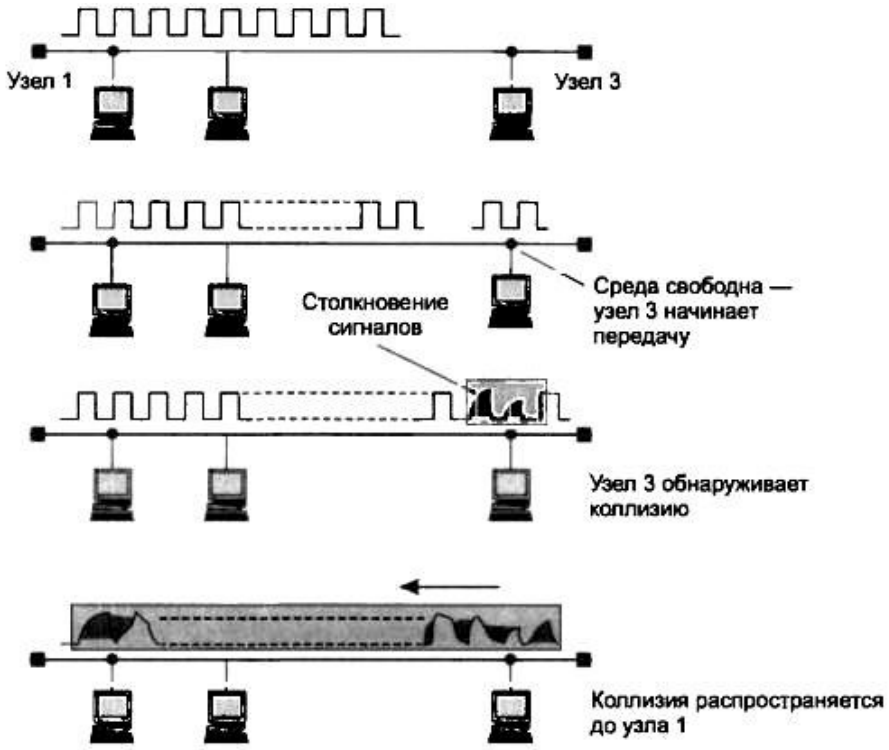


Рисунок 28 Схема возникновения и распространения коллизии

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабелях сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется факт обнаружения коллизии (Collision Detection, CD). Для повышения вероятности скорейшего обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего кадра (в произвольном месте, возможно, и не на границе байта) и усугубляет коллизию посылкой в сеть специальной последовательности из 32 бит, называемой jam-последовательностью.

После этого обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течение короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра. Случайная пауза выбирается по следующему алгоритму:

Пауза = L x (интервал отсрочки).

В технологии Ethernet интервал отсрочки выбран равным значению 512 битовых интервалов. Битовый интервал соответствует времени между появлением двух последовательных битов данных на кабеле; для скорости 10 Мбит/свеличина битового интервала равна 0,1 мкс, или 100 нс.

L представляет собой целое число, выбранное с равной вероятностью из диапазона [0, 2N], где N— номер повторной попытки передачи данного кадра: 1,2,..., 10. После 10-й попытки интервал, из которого выбирается пауза, не увеличивается.

Таким образом, случайная пауза в технологии Ethernet может принимать значения от 0 до 52,4 мс.

Если 16 последовательных попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр. Описанный алгоритм носит название усеченного экспоненциального двоичного алгоритма отсрочки.

Поведение сети Ethernet при значительной нагрузке, когда коэффициент использования среды растет и начинает приближаться к 1, в целом соответствует графикам, которые были приведены в главе 7 при анализе модели теории очередей M/M/1. Однако рост времени ожидания освобождения среды в сетях Ethernet начинается раньше, чем в модели M/M1. Это происходит из-за того, что модель M/M/1 является очень простой и не учитывает такой важной особенности Ethernet, как коллизии. Администраторы сетей Ethernet на разделяемой среде руководствуются простым эмпирическим правилом — коэффициент использования среды не должен превышать 30 %.

Для поддержки чувствительного к задержкам трафика сети Ethernet (и другие сети на разделяемой среде) могут применять только один метод поддержания характеристик QoS — недогруженный режим работы.

1.10 Лекция №11 (2 часа).

Тема: «Разновидности архитектуры сетей»

1.10.1 Вопросы лекции:

1. Эволюция Ethernet.
2. Спецификация Fast Ethernet.

1.10.2 Краткое содержание вопросов:

1. Эволюция Ethernet.

Ethernet, возникшая как сетевая технология с разделением среды передачи, а именно коаксиального кабеля, эволюционировала вместе с изменениями запросов пользователей. Соответствуя самым последним требованиям к кабельной проводке, стандарт Ethernet распространяется теперь на такие среды передачи данных, как оптическое волокно и неэкранированная витая пара. Побудительными мотивами перехода к этим средам стало быстрое и всепроникающее распространение локальных сетей в коммерческих, правительственных и другого рода организациях, а также потребность в эффективном и экономичном управлении и обслуживании данных сетей. Прежние же неструктурированные проводки из коаксиального кабеля не удовлетворяли этим требованиям.

Коммутация в Ethernet была разработана с целью расширения доступной для серверов и рабочих станций полосы пропускания. Появление недорогих коммутаторов для локальных сетей предопределило переход к разреженным и частным (выделенным) сетям с помощью микросегментации.

В начале 1960 ряд исследователей, многие из которых в дальнейшем участвовали в проекте ARPANET, видели громадный потенциал возможности компьютеров обмениваться данными друг с другом. Установленное в 1965 году соединение между компьютерами в Массачусеттском Институте Технологии и Университете Южной Калифорнии явилось эмбрионом Интернета.

Интернет был рожден в 1969 году, когда компьютеры четырех университетских центров США были соединены между собой. До середины 70-х, когда имя Интернет вошло в обиход, он носил имя ARPANET. По сравнению с традиционными телефонными сетями, основанными на коммутации каналов, технологии ARPANET использовали коммутацию пакетов - данных ограниченного объема, заключенных в "конверты" с указанием источника и получателя. Эта технология позволила существенно упростить архитектуру сети и повысить ее надежность.

Электронная почта (e-mail) и telnet (удаленный доступ в режиме терминала) появились в ARPANET в 1972, а ftp (обмен файлами) - годом позже. В то же десятилетие была разработана архитектура TCP/IP, которая была окончательно внедрена в начале 1980-х.

В 1986 году основой сети являлась национальная опорная сеть США - NSFNET с пропускной способностью в 56К. Основные приложения Сети - e-mail, ftp и telnet, стали стандартными на компьютерах того времени, что послужило существенному увеличению числа пользователей, особенно в университетах и научных центрах.

В то время как e-mail и ftp позволяли пользователям поддерживать деловые и социальные контакты и обмениваться информацией, а telnet - использовать удаленные вычислительные ресурсы, разрабатывалось все больше приложений, позволяющих каталогизировать и находить информацию в Сети. Сегодня мало кто помнит приложения Archie, WAIS или gopher, которые явились предтечей сегодняшнего вэба и поисковых машин.

1989 год ознаменовал рождение нового протокола, который стал основой системы WorldWideWeb- http. В поисках возможности объединения распределенных информационных ресурсов - в основном, документов, хранящихся на различных компьютерах, - Тим Бернерс-Ли (TimBerners-Lee), в то время сотрудник CERN, предложил идею гиперлинков, через которые пользователь может переходить с одного

документа на другой, находящийся, возможно, на другом компьютере и на другом континенте.

До начала 90-х Интернет в США в основном финансировался государством и его использование было доступно только для научно-образовательных учреждений. Подобная ситуация была и в Европе. С начала 90-х начинается коммерциализация Интернета и появляется все больше услуг, предлагаемых обычным пользователям. Соответственно, растет и число пользователей Интернета.

Де-регулирование и приватизация рынка телекоммуникаций в конце 1990-х, появление и широкое распространение персональных компьютеров и скоростных модемов открыло невиданные горизонты для развития Интернета. Рост пропускной способности стимулировал создание новых форм информационного контента, который в свою очередь требовал больших скоростей. Эта спираль инновации продолжается и сегодня, подстегнутая стремительным ростом мобильного Интернета и, как следствие, его размера и возможностей.

2. Спецификация FastEthernet.

Fast Ethernet — спецификация IEEE 802.3 u официально принятая 26 октября 1995 года определяет стандарт протокола канального уровня для сетей работающих при использовании как медного, так и волоконно-оптического кабеля со скоростью 100Мб/с. Новая спецификация является наследницей стандарта Ethernet IEEE 802.3, используя такой же формат кадра, механизм доступа к среде CSMA/CD и топологию звезда. Эволюция коснулась нескольких элементов конфигурации средств физического уровня, что позволило увеличить пропускную способность, включая типы применяемого кабеля, длину сегментов и количество концентраторов.

FastEthernet (Быстрый Ethernet) – высокоскоростная технология, предложенная фирмой 3Com для реализации сети Ethernet со скоростью передачи данных 100 Мбит/с, сохранившая в максимальной степени особенности 10-мегабитного Ethernet (Ethernet-10) и реализованная в виде стандарта 802.3u.

Основной целью при разработке технологии FastEthernet было обеспечение преемственности по отношению к 10-мегабитному Ethernet за счёт сохранения формата кадров и метода доступа CSMA/CD, что позволяет использовать прежнее программное обеспечение и средства управления сетями Ethernet. Одним из требований было также использование кабельной системы на основе витой пары категории 3, получившей на момент появления FastEthernet широкое распространение в сетях Ethernet-10. В связи с этим все отличия FastEthernet от Ethernet-10 сосредоточены на физическом уровне.

В FastEthernetпредусмотрены 3 варианта кабельных систем:

• многомодовый ВОК (используется 2 волокна);

• витая пара категории 5 (используется 2 пары);

• витая пара категории 3 (используется 4 пары).

Структура сети – иерархическая древовидная, построенная на концентраторах (как 10Base-T и 10Base-F), поскольку не предусматривалось использование коаксиального кабеля.

Диаметр сети Fast Ethernet, как показано в п.3.2.5, составляет немногим более 200 метров, что объясняется уменьшением времени передачи кадра минимальной длины в 10 раз в результате увеличения пропускной способности канала в 10 раз по сравнению с Ethernet-10. Тем не менее, возможно построение крупных сетей на основе технологии Fast Ethernet, благодаря появлению в начале 90-х годов прошлого века коммутаторов. При использовании коммутаторов протокол Fast Ethernet может работать в полнодуплексном режиме, в котором нет ограничений на общую длину сети, а остаются только ограничения на длину физических сегментов, соединяющих соседние устройства (адаптер – коммутатор или коммутатор – коммутатор).

Стандарт IEEE 802.3u определяет 3 спецификации физического уровня Fast Ethernet, несовместимых друг с другом:

• 100Base-TX – для передачи данных используются две неэкранированные пары UTP категории 5 или STP Type 1;

• 100Base-T4 – для передачи данных используются четыре неэкранированных пары UTP категорий 3, 4 или 5;

• 100Base-FX – для передачи данных используются два волокна многомодового ВОК.

Спецификации 100Base-TX и 100Base-FX.

Технологии 100Base-TX и 100Base-FX, несмотря на использование разных кабельных систем, имеют много общего с точки зрения построения и функционирования, в том числе, одинаковый метод логического кодирования – 4 B/5B при различных методах физического кодирования – MLT-3 в 100Base-TX и NRZI в 100Base-FX.

Кроме того, в технологии 100Base-TX имеется функция автопереговоров, обеспечивающая автоматическое определение скорости передачи (10 или 100 Мбит/с) между двумя связанными устройствами (СА, концентратор, коммутатор) путем посылки при подключении пачки специальных импульсов FLP – Fast Link Pulse burst – со стороны устройства, которое может работать на скорости 100 Мбит/с. Если встречное устройство не откликается на эти импульсы, это означает, что оно может работать только на скорости 10 Мбит/с, и первое устройство устанавливает режим передачи данных 10 Мбит/с.

Спецификация 100Base-T4.

К моменту появления Fast Ethernet большинство ЛВС Ethernet в качестве кабельной системы использовали неэкранированную витую пару категории 3. Желание сохранить кабельную систему 10-мегабитных ЛВС Ethernet обусловило применение специального метода логического кодирования – 8 B/6T, обеспечившего более узкий спектр сигнала, что при скорости 33 Мбит/с позволило уложиться в полосу 16 МГц витой пары категории 3.

При кодировании 8B/6T 8 бит заменяются 6-ю троичными цифрами. Длительность одной троичной цифры – 40 нс. Следовательно, один байт передается за 240 нс (6*40 нс), что соответствует скорости передачи в 33,3 Мбит/с. Для передачи данных используется 3 пары UTP категории 3 (3*33,3 Мбит/с = 100 Мбит/с), и еще одна пара используется для прослушивания несущей с целью обнаружения коллизий.

Скорость изменения сигнала на каждой паре составляет: 1/(40 нс) = 25 Мбод, что позволяет использовать витую пару категории 3/

Чтобы лучше понять работу и разобраться во взаимодействии элементов Fast Ethernet обратимся к рисунку 29.

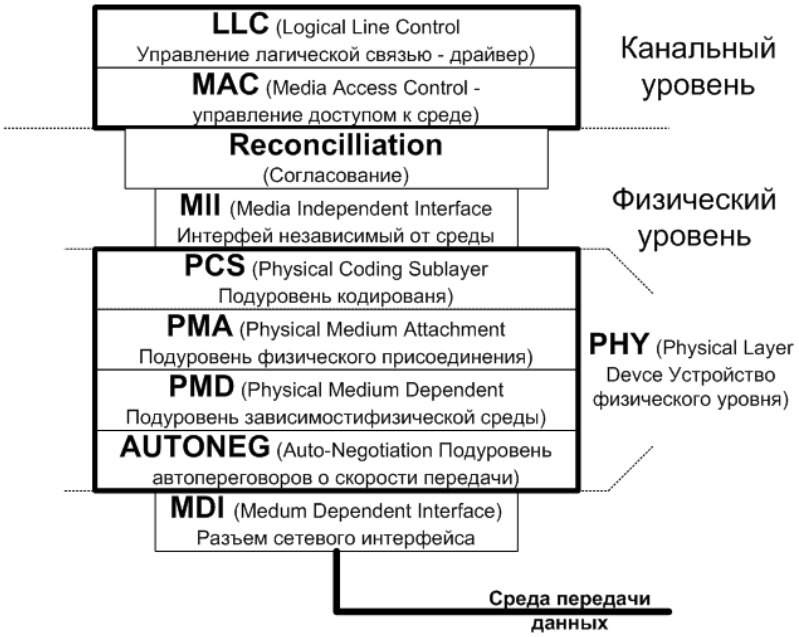


Рисунок 29. Система Fast Ethernet

В спецификации IEEE 802.3 u функции канального уровня разбиты на два подуровня: управления логической связью (LLC) и уровня доступа к среде (MAC), который будет рассмотрен ниже. LLC, функции которого определены стандартом IEEE

802.2, фактически обеспечивает взаимосвязь с протоколами более высокого уровня, (например, с IP или IPX), предоставляя различные коммуникационные услуги:

- **Сервис без установления соединения и подтверждений приема.** Простой сервис, который не обеспечивает управления потоком данных или контроля ошибок, а также не гарантирует правильную доставку данных.
- **Сервис с установлением соединения.** Абсолютно надежный сервис, который гарантирует правильную доставку данных за счет установления соединения с системой-приемником до начала передачи данных и использования механизмов контроля ошибок и управления потоком данных.
- **Сервис без установления соединения с подтверждениями приема.** Средний по сложности сервис, который использует сообщения подтверждения приема для обеспечения гарантированной доставки, но не устанавливает соединения до передачи данных.

На передающей системе данные, переданные вниз от протокола Сетевого уровня, вначале инкапсулируются подуровнем LLC. Стандарт называет их Protocol Data Unit (PDU, протокольный блок данных). Когда PDU передается вниз подуровню MAC, где снова обрамляется заголовком и постинформацией, с этого момента технически его можно назвать кадром. Для пакета Ethernet это означает, что кадр 802.3 помимо данных Сетевого уровня содержит трехбайтовый заголовок LLC. Таким образом, максимально допустимая длина данных в каждом пакете уменьшается с 1500 до 1497 байтов.

Заголовок LLC состоит из трех полей:

- **DSAP** (1 байт) *Destination Service Access Point* — точка доступа к сервису системы — получателя указывает, в каком месте буферов памяти системы-получателя следует разместить данные пакета.
- **SSAP** (1 байт) *Source Service Access Point* — точка доступа к сервису системы — источника выполняет такие же функции для источника данных, размещенных в пакете, на передающей системе.
- **Поле управления** (1 или 2 байта) указывает на тип сервиса, необходимого для данных в PDU и функций пакета. В зависимости от того, какой сервис нужно предоставить, поле управления может быть длиной 1 или 2 байта.

Принимающей системе необходимо определить, какой из протоколов Сетевого уровня должен получить входящие данные. В пакетах 802.3 в рамках PDU LLC применяется еще один протокол, называемый *Sub -Network Access Protocol (SNAP, протокол доступа к подсетям).*

Заголовок SNAP имеет длину 5 байт и располагается непосредственно после заголовка LLC в поле данных кадра 802.3, как показано на рисунке. Заголовок содержит два поля.

Код организации. Идентификатор организации или производителя — это 3-байтовое поле, которое принимает такое же значение, как первые 3 байта MAC-адреса отправителя в заголовке 802.3.

Локальный код. Локальный код — это поле длиной 2 байта, которое функционально эквивалентно полю Ethertype в заголовке Ethernet II.

Подуровень согласования

Как было сказано ранее Fast Ethernet это эволюционировавший стандарт. MAC рассчитанный на интерфейс AUI, необходимо преобразовать для интерфейса MII, используемого в Fast Ethernet, для чего и предназначен этот подуровень.

Управление доступом к среде (MAC)

Каждый узел в сети Fast Ethernet имеет контроллер доступа к среде **(Media AccessController** — MAC). MAC имеет ключевое значение в Fast Ethernet и имеет три назначения:

- определяет, когда узел может передать пакет;
- пересылает кадры уровню PHY для преобразования в пакеты и передачи в среду;
- получает кадры из уровня PHY и передает обрабатывающему их программному обеспечению (протоколам и приложениям).*

Самым важным из трех назначений MAC является первое. Для любой сетевой технологии, которая использует общую среду, правила доступа к среде, определяющие, когда узел может передавать, являются ее основной характеристикой. Разработкой правил доступа к среде занимаются несколько комитетов IEEE. Комитет 802.3, часто именуемый комитетом Ethernet, определяет стандарты на ЛВС, в которых используются правила под названием **CSMA/ CD** (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов).

CSMS/ CD являются правилами доступа к среде как для Ethernet, так и для Fast Ethernet. Именно в этой области две технологии полностью совпадают.

Поскольку все узлы в Fast Ethernet совместно используют одну и ту же среду, передавать они могут лишь тогда, когда наступает их очередь. Определяют эту очередь правила CSMA/ CD.

CSMA/ CD

Контроллер MAC Fast Ethernet, прежде чем приступить к передаче, прослушивает несущую. Несущая существует лишь тогда, когда другой узел ведет передачу. Уровень PHY определяет наличие несущей и генерирует сообщение для MAC. Наличие несущей говорит о том, что среда занята и слушающий узел (или узлы) должны уступить передающему.

Устройство физического уровня (PHY)

Поскольку Fast Ethernet может использовать различный тип кабеля, то для каждой среды требуется уникальное предварительное преобразование сигнала. Преобразование также требуется для эффективной передачи данных: сделать передаваемый код устойчивым к помехам, возможным потерям, либо искажениям отдельных его элементов (бодов), для обеспечения эффективной синхронизации тактовых генераторов на передающей или приемной стороне.

Подуровень кодирования (PCS)

Кодирует/декодирует данные поступающие от/к уровня MAC с использованием алгоритмов 4B/5B или8B/6T.

Подуровни физического присоединения и зависимости от физической среды (PMA и PMD)

Подуровни PMA и PMD осуществляют связь между подуровнем PSC и интерфейсом MDI, обеспечивая формирование в соответствии с методом физического кодирования: NRZI или MLT-3.

Подуровень автопереговоров (AUTONEG)

Подуровень автопереговоров позволяет двум взаимодействующим портам автоматически выбирать наиболее эффективный режим работы: дуплексный или полудуплексный 10 или 100 Мб/с.

1.11 Лекция №12 (2 часа).

Тема: «Способы модуляции»

1.11.1 Вопросы лекции:

1. Модуляция при передаче аналоговых сигналов.
2. Модуляция при передаче дискретных сигналов.

1.11.2 Краткое содержание вопросов:

1. Модуляция при передаче аналоговых сигналов.

Передача данных осуществляется в виде физических сигналов различной природы (электрические, оптические, радиоволны) в зависимости от среды передачи. Для обеспечения качественной передачи используются различные способы преобразования данных, представляемых в виде непрерывных или дискретных первичных сигналов, в линейные физические сигналы (непрерывные или дискретные), передаваемые по линии связи.

Процесс преобразования непрерывных сигналов и их представление в виде физических сигналов для качественной передачи по каналам связи называется модуляцией.

Модуляция может осуществляться (рис.30):

• на основе непрерывного (аналогового) высокочастотного синусоидального сигнала, называемого несущей (аналоговая модуляция);

• на основе дискретного (цифрового) сигнала в виде импульсов (импульсная или цифровая модуляция).

Аналоговая модуляция - преобразование непрерывного низкочастотного сигнала x(t) (рис.30,а) в непрерывный высокочастотный сигнал y(t), называемый несущей и обладающий более высокими характеристиками в отношении дальности передачи и затухания. Аналоговая модуляция может быть реализована двумя способами:

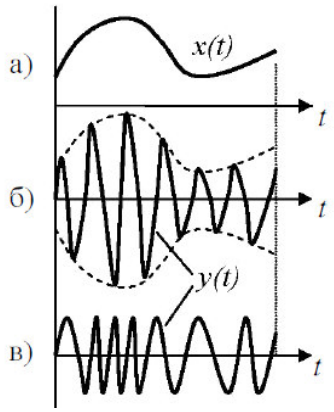


Рисунок 30. Аналоговая модуляция

1) амплитудная модуляция, при которой амплитуда высокочастотного сигнала y(t) изменяется в соответствии с исходной функцией x(t) так, как это показано на рис.30,б: огибающая амплитуды несущей повторяет форму исходной функции x(t) ;

2) частотная модуляция (рис.30,в), при которой в соответствии с исходной функцией x(t) изменяется частота несущей - чем больше значение x(t), тем больше частота несущей y(t)

Аналоговая модуляция используется в радиовещании при работе множества радиостанций в одной общей среде передачи (радиоэфире): амплитудная модуляция для работы радиостанций в АМ-диапазоне (Amplitude Modulation) и частотная модуляция для работы радиостанций в FM — диапазоне (Frequence Modulatin).

Использование цифровых каналов связи для передачи телефонных данных (речевого сигнала) в начале 60-х годов прошлого века потребовало разработки методов преобразования непрерывных сигналов в дискретные, таких как:

1) амплитудно-импульсная модуляция;

2) импульсно-кодовая модуляция.

Амплитудно-импульсная модуляция (АИМ) (Pulse Amplitude Modulation - PAM) заключается в преобразовании непрерывного сигнала в совокупность дискретных сигналов (импульсов) с определенной амплитудой. Для этого исходная непрерывная функция x(t) подвергается дискретизации (квантуется) по времени так, как это показано на рис.31,а.

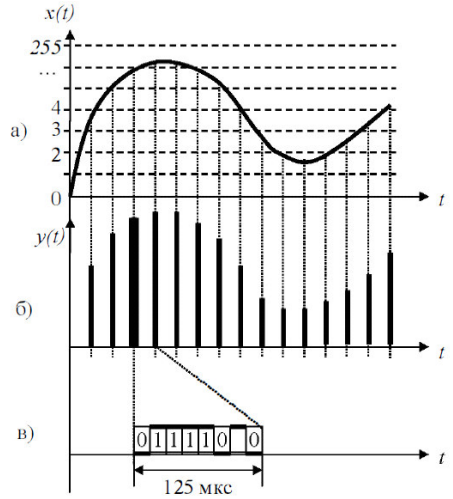


Рисунок 31. АИМ

Частота дискретизации по времени определяется в соответствии с теоремой Котельникова, которая гласит, что для восстановления без потерь непрерывного сигнала, представленного в дискретном виде, частота дискретизации должна удовлетворять условию:, где - верхняя частота передаваемого сигнала x(t) . В полученные таким образом дискретные моменты времени передаются импульсы y(t) , амплитуда которых пропорциональна значениям функции x(t) в эти же моменты времени (рис.31,б).

Существенным недостатком АИМ при передаче оцифрованных данных по каналу связи является сложность корректного восстановления функции x(t) на приёмном конце, что обусловлено непропорциональным изменением (затуханием) амплитуд разных

импульсов y(t) в процессе передачи по каналу связи. В связи с этим, более широкое распространение получил другой метод передачи непрерывных данных в дискретном виде - импульсно-кодовая модуляция.

Импульсно-кодовая модуляция (ИКМ) (Pulse Code Modulation - PCM) - метод модуляции, при котором аналоговый сигнал кодируется сериями импульсов, представляющими собой цифровые коды амплитуд в точках отсчета аналогового сигнала.

Для этого исходный сигнал подвергается дискретизации (квантуется) по двум координатам:

• по оси абсцисс - дискретизация по времени;

• по оси ординат - дискретизация по уровню.

Дискретизация по времени, как и в случае АИМ, выполняется в соответствии с теоремой Котельникова. Поскольку ИКМ первоначально разрабатывалась для передачи телефонных данных (голоса) по телефонным каналам, имеющим резко ограниченную полосу пропускания в интервале от 300 Гц до 3400 Гц, то в соответствии с теоремой Котельникова частота дискретизации должна быть больше, чем 6800 Гц. Стандартом была рекомендована частота дискретизации 8000 Гц. Таким образом, амплитуда аналогового сигнала измеряется 8000 раз в секунду, то есть каждые 125 мкс.

Для качественного восстановления аналогового сигнала (голоса) достаточно иметь 256 уровней дискретизации (рис.31,а), что позволяет передавать в каждый момент времени значение амплитуды (номер уровня) сигнала с помощью 8-разрядного цифрового кода (8 битов) (рис.31,в).

Таким образом, результирующий дискретный поток данных передается со скоростью 8000 [раз в секунду]*8 [бит] = 64 000 бит/с, то есть для передачи оцифрованного голоса требуется канал связи с пропускной способностью 64 кбит/с.

Для уменьшения требуемой для передачи оцифрованного голоса пропускной способности канала связи применяется модифицированный метод ИКМ - адаптивная дифференциальная импульсно-кодовая модуляция (АДИКМ).

Термин «дифференциальная (разностная)» означает, что по каналу связи передаётся не значение амплитуды, а разность между текущим значением непрерывного сигнала в точке квантования и предыдущим.

Поскольку скорость изменения исходного аналогового сигнала меньше частоты квантования, то вероятность большого различия между соседними амплитудами чрезвычайно мала, и для кодирования этой разности достаточно 4-х бит, позволяющих закодировать эту разность в интервале от О до 15. Тогда при условии, что частота

квантования по времени составляет 8000 раз в секунду, получим скорость передачи 8000*4 =32 кбит/с, что вдвое меньше стандартной скорости ИКМ.

Более сложным вариантом дифференциальной импульсно-кодовой модуляции является кодирование с предсказанием, при котором кодируется и передаётся разница между реальным и предсказанным на основе нескольких предыдущих отсчётов значением сигнала. Это позволяет ещё больше уменьшить количество битов для кодирования одного замера сигнала и, следовательно, уменьшить требование к пропускной способности канала связи. Адаптивность модуляции заключается в динамической подстройке шага квантования разницы по предыдущим значениям.

Аналоговая модуляция является таким способом физического кодирования, при котором информация кодируется изменением амплитуды, частоты или фазы синусоидального сигнала несущей частоты. Основные способы аналоговой модуляции показаны на рис. На диаграмме показана последовательность бит исходной информации, представленная потенциалами высокого уровня для логической единицы и потенциалом нулевого уровня для логического нуля. Такой способ кодирования называется потенциальным кодом, который часто используется при передаче данных между блоками компьютера.

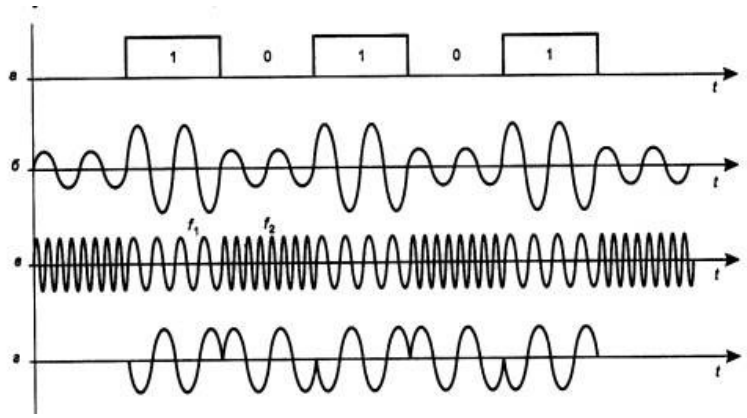


Рисунок 32. Различные типы модуляции (а - исходная информация, б- амплитудная модуляция, в - частотная модуляция, г - фазовая модуляция).

При **амплитудной модуляции** для логической единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля - другой. Этот способ редко используется в чистом виде на практике из-за низкой помехоустойчивости, но часто применяется в сочетании с другим видом модуляции - фазовой модуляцией.

При **частотной модуляции** значения 0 и 1 исходных данных передаются синусоидами с различной частотой - f_0 и f_1. Этот способ модуляции не требует сложных

схем в модемах и обычно применяется в низкоскоростных модемах, работающих на скоростях 300 или 1200 бит/с.

При **фазовой модуляции** значениям данных 0 и 1 соответствуют сигналы одинаковой частоты, нос различной фазой, например 0 и 180 градусов или 0,90,180 и 270 градусов.

В скоростных модемах часто используются комбинированные методы модуляции, как правило, амплитудная в сочетании с фазовой.

2. Модуляция при передаче дискретных сигналов.

Процесс представления дискретных (цифровых) данных в виде непрерывного высокочастотного синусоидального сигнала (несущей) по своей сути является аналоговой модуляцией дискретных данных. Однако, для того чтобы его отличать от аналоговой модуляции непрерывных данных, такое преобразование часто называют манипуляцией.

Манипуляция применяется для передачи дискретных данных (сигналов) в виде непрерывных сигналов по каналам с узкой полосой частот, например по телефонным каналам, имеющим ограниченную полосу пропускания в 3100 Гц, и реализуется с помощью модемов.

Компьютерные данные – двоичные «1» и «0» – обычно изображаются в виде потенциалов соответственно высокого и низкого уровней (рис.33,а). Такой метод представления двоичных данных является наиболее естественным и простым и называется потенциальным кодированием.

Время, затрачиваемое на передачу одного бита («1» или «0»), называется битовым интервалом. Длительность tb битового интервала связана с пропускной способностью канала связи C (скоростью передачи) зависимостью: tb□ 1/ C .

При потенциальном кодировании скорость модуляции B численно совпадает с пропускной способностью канала :B [бод]=C [бит/с].

Например, для канала связи с пропускной способностью =10 Мбит/с длительность битового интервала = 100 нс, а скорость модуляции=10 Мбод Для передачи двоичных данных могут использоваться следующие методы манипуляции:

• амплитудная манипуляция (Amplitude Shift Keying, ASK): для представления «1» и «0» используются разные уровни амплитуды высокочастотной несущей (рис.33,б); из-за низкой помехоустойчивости этот метод обычно применяется в сочетании с другими методами, например с фазовой манипуляцией;

• частотная манипуляция (FrequencyShiftKeying, FSK): значения

«0» и «1» передаются синусоидами с различной частотой (рис.33,в); этот метод прост в реализации и обычно применяется в низкоскоростных модемах;

• фазовая манипуляция (Phase Shift Keying, PSK): значениям «0» и «1» соответствуют синусоиды одинаковой частоты и с одинаковой амплитудой, но с различной фазой, например 0 и 180 градусов (рис.33,г).

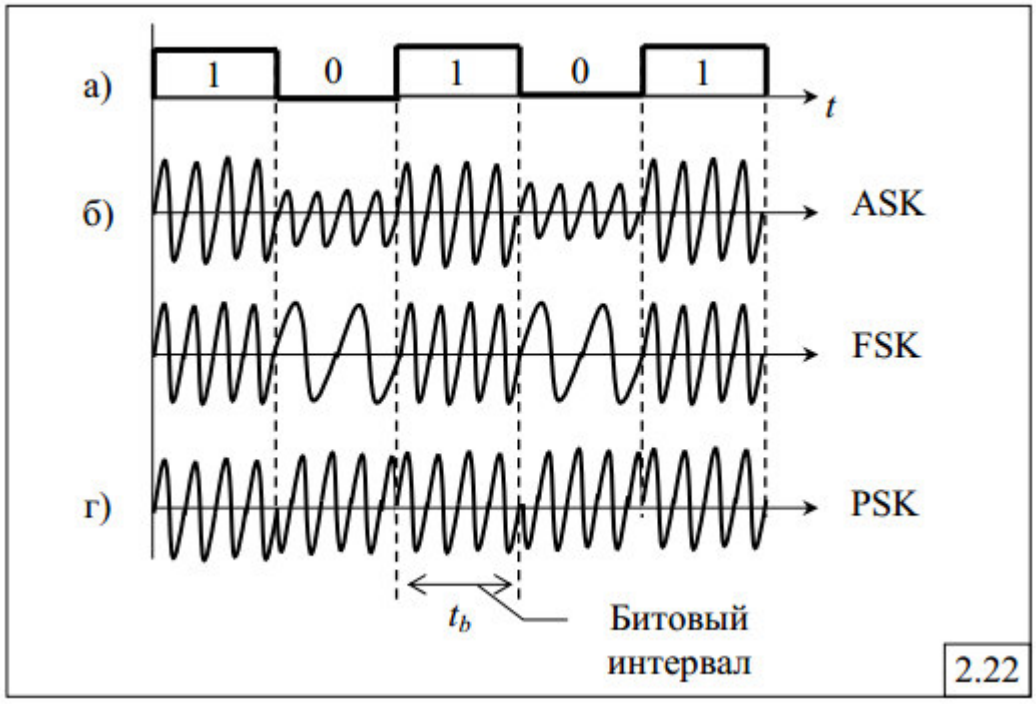


Рисунок 33. Дискретная модуляция

Дискретные способы модуляции основаны на дискретизации непрерывных процессов как по амплитуде, так и по времени. Рассмотрим принципы искретной модуляции на примере *импулъсно-кодовой модуляции, ИКМ (Pulse Amplitude Modulation, PAM)*, которая широко применяется в цифровой телефонии.

Амплитуда исходной непрерывной функции измеряется с заданным периодом - за счет этого происходит дискретизация по времени. Затем каждый замер представляется в виде двоичного числа определенной разрядности, что означает дискретизацию по значениям функции - непрерывное множество возможных значений амплитуды заменяется дискретным множеством ее значений. Устройство, которое выполняет подобную функцию, называется *аналого-цифровым преобразователем (АЦП)*. После этого замеры передаются по каналам связи в виде последовательности единиц и нулей. При этом применяются те же методы кодирования, что и в случае передачи изначально дискретной информации, то есть, например, методы, основанные на коде B8ZS или 2B 1Q.

На приемной стороне линии коды преобразуются в исходную последовательность бит, а специальная аппаратура, называемая *цифро-аналоговым преобразователем (ЦАП)*, производит демодуляцию оцифрованных амплитуд непрерывного сигнала, восстанавливая исходную непрерывную функцию времени.

Дискретная модуляции основана на *теории отображения Найквиста - Котельникова*. В соответствии с этой теорией, аналоговая непрерывная функция, переданная в виде последовательности ее дискретных по времени значений, может быть точно восстановлена, если частота дискретизации была в два или более раз выше, чем частота самой высокой гармоники спектра исходной функции.

Если это условие не соблюдается, то восстановленная функция будет существенно отличаться от исходной.

Преимуществом цифровых методов записи, воспроизведения и передачи аналоговой информации является возможность контроля достоверности считанных с носителя или полученных по линии связи данных. Для этого можно применять те же методы, которые применяются для компьютерных данных (и рассматриваются более подробно далее), - вычисление контрольной суммы, повторная передача искаженных кадров, применение самокорректирующихся кодов.

На практике обычно используются комбинированные методы модуляции, обеспечивающие более высокие скорости передачи и лучшую помехозащищённость. Например, метод квадратурной амплитудной модуляции (Quadrature Amplitude Modulation, QAM) основан на сочетании фазовой модуляции с 8 значениями величин сдвига фазы и амплитудной модуляции с 4 уровнями амплитуды. Распознавание ошибок при передаче осуществляется за счёт избыточности кодирования, заключающейся в использовании не всех 32-х возможных комбинаций сигнала.

1.12 Лекция №13,14 (4 часа).

Тема: «Высокоскоростные магистрали»

1.12.1 Вопросы лекции:

1. Технология FDDI.
2. Технология ATM.

1.12.2 Краткое содержание вопросов:

1. Технология FDDI.

Технология FDDI во многом основывается на технологии TokenRing, развивая и совершенствуя ее основные идеи. Разработчики технологии FDDI ставили перед собой в качестве наиболее приоритетных следующие цели:

• Повысить битовую скорость передачи данных до 100 Мб/с;

• Повысить отказоустойчивость сети за счет стандартных процедур восстановления ее после отказов различного рода - повреждения кабеля, некорректной работы узла, концентратора, возникновения высокого уровня помех на линии и т.п.;

• Максимально эффективно использовать потенциальную пропускную способность сети как для асинхронного, так и для синхронного трафиков.

Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец - это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля первичного (Primary) кольца, поэтому этот режим назван режимом Thru - "сквозным" или "транзитным". Вторичное кольцо (Secondary) в этом режиме не используется.

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется со вторичным (рисунок 34), образуя вновь единое кольцо. Этот режим работы сети называется Wrap, то есть "свертывание" или "сворачивание" колец. Операция свертывания производится силами концентраторов и/или сетевых адаптеров FDDI. Для упрощения этой процедуры данные по первичному кольцу всегда передаются против часовой стрелки, а по вторичному - по часовой. Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

В стандартах FDDI отводится много внимания различным процедурам, которые позволяют определить наличие отказа в сети, а затем произвести необходимую реконфигурацию. Сеть FDDI может полностью восстанавливать свою работоспособность в случае единичных отказов ее элементов. При множественных отказах сеть распадается на несколько не связанных сетей.

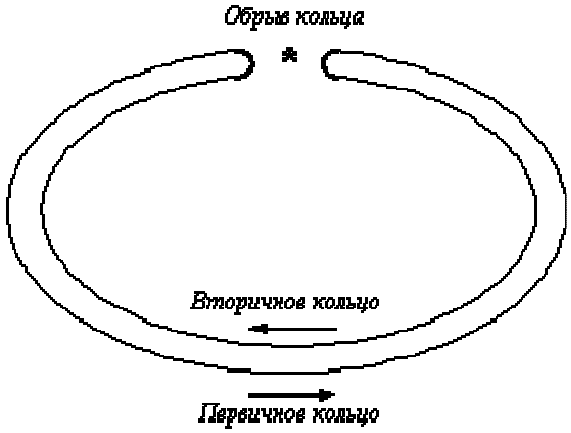


Рис. 34. Реконфигурация колец FDDI при отказе

Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа сетей TokenRing и также называется методом маркерного (или токенного) кольца - tokenring (рисунок 35, а).

Станция может начать передачу своих собственных кадров данных только в том случае, если она получила от предыдущей станции специальный кадр - токен доступа (рисунок 35, б). После этого она может передавать свои кадры, если они у нее имеются, в течение времени, называемого временем удержания токена - TokenHoldingTime (THT). После истечения времени THT станция обязана завершить передачу своего очередного кадра и передать токен доступа следующей станции. Если же в момент принятия токена у станции нет кадров для передачи по сети, то она немедленно транслирует токен следующей станции. В сети FDDI у каждой станции есть предшествующий сосед (upstreamneighbor) и последующий сосед (downstreamneighbor), определяемые ее физическими связями и направлением передачи информации.

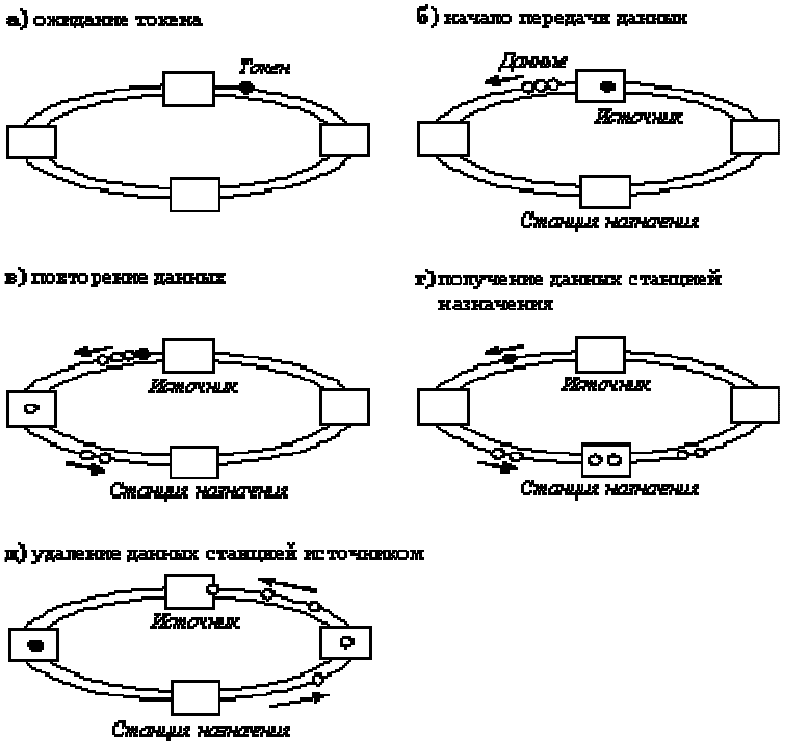


Рисунок 35. Обработка кадров станциями кольца FDDI

Каждая станция в сети постоянно принимает передаваемые ей предшествующим соседом кадры и анализирует их адрес назначения. Если адрес назначения не совпадает с ее собственным, то она транслирует кадр своему последующему соседу. Этот случай приведен на рисунке (рисунок 35, в). Нужно отметить, что, если станция захватила токен и передает свои собственные кадры, то на протяжении этого периода времени она не транслирует приходящие кадры, а удаляет их из сети.

Если же адрес кадра совпадает с адресом станции, то она копирует кадр в свой внутренний буфер, проверяет его корректность (в основном по контрольной сумме), передает его поле данных для последующей обработки протоколу лежащего выше над FDDI уровня (например, IP), а затем передает исходный кадр по сети последующей станции (рисунок 35, г). В передаваемом в сеть кадре станция назначения отмечает три признака: распознавания адреса, копирования кадра и отсутствия или наличия в нем ошибок.

После этого кадр продолжает путешествовать по сети, транслируясь каждым узлом. Станция, являющаяся источником кадра для сети, ответственна за то, чтобы удалить кадр из сети, после того, как он, совершив полный оборот, вновь дойдет до нее (рисунок 35, д). При этом исходная станция проверяет признаки кадра, дошел ли он до станции назначения и не был ли при этом поврежден. Процесс восстановления информационных кадров не входит в обязанности протокола FDDI, этим должны заниматься протоколы более высоких уровней.

На рисунке 36 приведена структура протоколов технологии FDDI в сравнении с семиуровневой моделью OSI. FDDI определяет протокол физического уровня и протокол подуровня доступа к среде (MAC) канального уровня. Как и многие другие технологии локальных сетей, технология FDDI использует протокол 802.2 подуровня управления каналом данных (LLC), определенный в стандартах IEEE 802.2 и ISO 8802.2. FDDI использует первый тип процедур LLC, при котором узлы работают в дейтаграммном режиме - без установления соединений и без восстановления потерянных или поврежденных кадров.

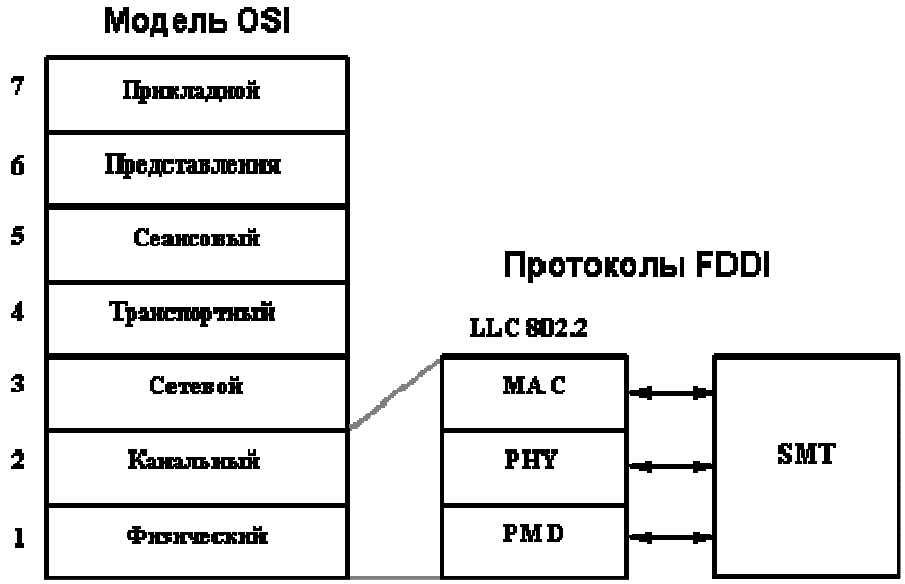


Рисунок 36. Структура протоколов технологии FDDI

Физический уровень разделен на два подуровня: независимый от среды подуровень PHY (Physical), и зависящий от среды подуровень PMD (PhysicalMediaDependent). Работу всех уровней контролирует протокол управления станцией SMT (StationManagement).

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 многомодовому оптоволоконному кабелю 62.5/125 мкм;

• Требования к оптическим обходным переключателям (opticalbypassswitches) и оптическим приемопередатчикам;

• Параметры оптических разъемов MIC (MediaInterfaceConnector), их маркировка;

• Длина волны в 1300 нанометров, на которой работают приемопередатчики;

• Представление сигналов в оптических волокнах в соответствии с методом NRZI.

Спецификация TP-PMD определяет возможность передачи данных между станциями по витой паре в соответствии с методом MLT-3. Спецификации уровней PMD и TP-PMD уже были рассмотрены в разделах, посвященных технологии FastEthernet.

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 со схемой 4B/5B;

• правила тактирования сигналов;

• требования к стабильности тактовой частоты 125 МГц;

• правила преобразования информации из параллельной формы в последовательную.

Уровень MAC ответственен за управление доступом к сети, а также за прием и обработку кадров данных. В нем определены следующие параметры:

• Протокол передачи токена;

• Правила захвата и ретрансляции токена;

• 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;

• Процедуры инициализации кольца.

Отказоустойчивость сетей FDDI обеспечивается за счет управления уровнем SMT другими уровнями: с помощью уровня PHY устраняются отказы сети по физическим причинам, например, из-за обрыва кабеля, а с помощью уровня MAC - логические отказы сети, например, потеря нужного внутреннего пути передачи токена и кадров данных между портами концентратора.

Есть два основных способа подключения компьютеров к сети FDDI:
непосредственно, а также через мосты или маршрутизаторы к сетям других протоколов.

Непосредственное подключение.

Этот способ используется, как правило, для подключения к сети FDDI файловых, архивационных и других серверов, средних и больших ЭВМ, то есть ключевых сетевых компонентов, являющихся главными вычислительными центрами, предоставляющими сервис для многих пользователей и требующих высоких скоростей ввода-вывода по сети.

Аналогично можно подключить и рабочие станции. Однако, поскольку сетевые адаптеры для FDDI весьма дороги, этот способ применяется только в тех случаях, когда высокая скорость обмена по сети является обязательным условием для нормальной работы приложения. Примеры таких приложений: системы мультимедиа, передача видео и звуковой информации.

Для подключения к сети FDDI персональных компьютеров применяются специализированные сетевые адаптеры, которые обычным образом вставляются в один из свободных слотов компьютера. Такие адаптеры производятся фирмами: 3Com, IBM, Microdyne, Network Peripherials, SysKonnect и др. На рынке имеются карты под все распространенные шины - ISA, EISA и Micro Channel; есть адаптеры для подключения станций классов A или B для всех видов кабельной системы - волоконно-оптической, экранированной и неэкранированной витых пар.

Все ведущие производители UNIX машин (DEC, Hewlett-Packard, IBM, Sun Microsystems и другие) предусматривают интерфейсы для непосредственного подключения к сетям FDDI.

Подключение через мосты и маршрутизаторы.

Мосты (bridges) и маршрутизаторы (routers) позволяют подключить к FDDI сети других протоколов, например, Token Ring и Ethernet. Это делает возможным экономичное подключение к FDDI большого числа рабочих станций и другого сетевого оборудования как в новых, так и в уже существующих ЛВС.

Конструктивно мосты ит маршрутизаторы изготавливаются в двух вариантах - в законченном виде, не допускающем дальнейшего аппаратного наращивания или переконфигурации (так называемые standalone-устройства), и в виде модульных концентраторов.

Примером standalone-устройств являются: Router BR фирмы Hewlett-Packard и EIFO Client/Server Switching Hub фирмы Network Peripherals.

Модульные концентраторы применяются в сложных больших сетях в качестве центральных сетевых устройств. Концентратор представляет собой корпус с источником питания и с коммуникационной платой. В слоты концентратора вставляются сетевые коммуникационные модули. Модульная конструкция концентраторов позволяет легко

собрать любую конфигурацию ЛВС, объединить кабельные системы различных типов и протоколов. Оставшиеся свободными слоты можно использовать для дальнейшего наращивания ЛВС.

Концентраторы производятся многими фирмами: 3Com, Cabletron, Chipcom, Cisco, Gandalf, Lannet, Proteon, SMC, SynOptics, Wellfleet и другими.

Концентратор — это центральный узел ЛВС. Его отказ может привести к остановке всей сети, или, по крайней мере, значительной её части. Поэтому большинство фирм, производящих концентраторы, принимают специальные меры для повышения их отказоустойчивости. Такими мерами являются резервирование источников питания в режиме разделения нагрузки или горячего резервирования, а также возможность смены или доустановки модулей без отключения питания (hot swap).

Для того чтобы снизить стоимость концентратора, все его модули запитываются от общего источника питания. Силовые элементы источника питания являются наиболее вероятной причиной его отказа. Поэтому резервирование источника питания существенно продлевает срок безотказной работы. При инсталляции каждый из источников питания концентратора может быть подключен к отдельному источнику бесперебойного питания (UPS) на случай неисправностей в системе электроснабжения. Каждый из UPS желательно подключить к отдельным силовым электрическим сетям от разных подстанций.

Возможность смены или доустановки модулей (часто включая и источники питания) без отключения концентратора позволяет провести ремонт или расширение сети без прекращения сервиса для тех пользователей, сетевые сегменты которых подключены к другим модулям концентратора.

В следующей таблице представлены результаты сравнения технологии FDDI с технологиями Ethernet и TokenRing.

Характеристика	**FDDI**	**EthernetTokenRing**
Битовая скорость	100 Мб/с	10 Мб/с16 Мб/с
Топология	Двойное кольцо деревьев	Шина/звездаЗвезда/кольцо
Метод доступа	Доля от времени оборота токена	CSMA/CDПриоритетная система резервирования
Среда передачи данных	Многомодовое оптоволокно, неэкранированная	Толстый коаксиал, тонкий коаксиал, витая пара, оптоволокно. Экранированная и неэкранированная

	витая пара	витая пара, оптоволокно.
Максимальная длина сети (без мостов)	200 км (100 км на кольцо)	2500 м1000 м
Максимальное расстояние между узлами	2 км (-11 dB потерь между узлами)	2500 м100 м
Максимальное количество узлов	500 (1000 соединений)	1024260 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

2. Технология ATM.

Технология ATM является наиболее перспективным решением задачи переноса разнородной информации в широкополосных цифровых сетях с интеграцией служб. Это - специфический, подобный пакетному, метод переноса информации, использующий принцип асинхронного временного мультиплексирования.

Метод ATM является ориентированным на соединения: любой передаче информации предшествует организация виртуального соединения (коммутируемого или постоянного) между отправителем и получателем данных, что впоследствии упрощает процедуры маршрутизации. Данные перед их передачей по каналам связи делятся на участки длиной 48 байт. К ним добавляется заголовок (5 байт). Образуются ячейки, которые передаются с использованием виртуальных каналов, т.е. имеющих идентификатор логических каналов, организуемых между двумя устройствами для установления связи. В одном физическом канале связи, как правило, передаются совместно ячейки, принадлежащие множеству различных виртуальных каналов. Ячейки, поступающие от различных комплектов оконечного оборудования данных, объединяются в канале связи, образуя групповой сигнал, и коммутируются в узлах сети.

По сравнению с коммутацией пакетов, где пакеты могут иметь различные размеры с различными расстояниями между ними, ячейки ATM имеют строго фиксированную длину, кратную байту, и следуют друг за другом без перерывов. Это облегчает процедуры обработки сигнала, что позволяет повысить скорость передачи информации и предоставляет возможности широкополосной связи. В отличие от коммутации каналов с

временным уплотнением ячейки предоставляются пользователям только на время передачи информации. При отсутствии необходимости передачи информации пользователь не занимает ресурсы сети связи, что повышает эффективность их использования. Отсюда происходит название метода: термин “асинхронный” означает, что ячейки, принадлежащие одному соединению, поступают в канал связи нерегулярно, и временные интервалы предоставляются источнику сообщений в соответствии с его реальными потребностями.

Небольшая длина ячейки позволяет легко перемежать ячейки, используемые для различных приложений, таких как передача данных, речи и видеоизображений. Высокая скорость дает возможность передавать информацию в реальном масштабе времени.

Контрольные функции, такие как распознавание типа сообщения, подтверждение факта получения сообщения принимающим терминалом, выявление ошибок при передаче информации, управление повторной передачей и т.д. с целью упрощения процедур обработки ячеек промежуточными узлами связи переданы протоколам верхних уровней.

Общая композиция протоколов включает физический уровень, уровень ATM, уровень адаптации (AAL - ATMAdaptationLayer), который зависит от вида предоставляемой услуги, и верхние уровни.

Физический уровень соответствует традиционному первому уровню эталонной модели взаимодействия открытых систем и регламентирует физическую среду переноса информации. Кроме того он обеспечивает функции идентификации границ ячеек, обнаружения и исправления ошибок в заголовках.

Уровень ATM служит для мультиплексирования/ демультиплексирования ячеек, генерации заголовков ячеек, выделения информационного поля и прозрачный его перенос. Никакая обработка информационного поля (например, контроль на наличие ошибок) уровнем ATM не выполняется. Граница между уровнем ATM и уровнем адаптации соответствует границе между функциями, относящимися к заголовку, и функциями, относящимися к информационному полю.

Уровень AAL поддерживает функции протоколов верхних уровней, обеспечивает адаптацию с ними функций передачи уровня ATM, а также соединения между ATM и не-ATM интерфейсами. Примерами функций данного уровня являются обнаружение информационных блоков, поступающих с верхнего уровня, их сегментация на передающем конце и преобразование исходного цифрового сигнала в ячейки ATM, восстановление исходной информации из ячеек ATM на приемном конце, направление информационных блоков к верхнему уровню, компенсация переменной величины задержки в сети ATM для звуковых сигналов, обработка частично заполненных ячеек,

действия при потере ячеек и т.д. Любая специфическая информация уровня адаптации (например, длина поля данных, отметки времени, порядковый номер), которая должна быть передана между взаимодействующими уровнями адаптации, содержится в информационном поле ячейки АТМ.

Телекоммуникационная сеть, использующая технологию АТМ, состоит из набора коммутаторов, связанных между собой. Коммутаторы АТМ поддерживают два вида интерфейсов: интерфейс “пользователь - сеть” (UNI - user-networkinterface) и интерфейс “сеть - узел сети” (NNI - network-networkinterface). UNI соединяет оконечные системы АТМ (рабочие станции, маршрутизаторы и др.) с коммутатором АТМ, тогда как NNI может быть определен как интерфейс, соединяющий два коммутатора АТМ.

В таблице показан формат ячейки АТМ в соответствии со стандартом UNI.

VCIL	Control	HCS	AL	ДАННЫЕ
Заголовок 5 байт			Поле данных 48 байт	

VCIL - идентификатор постоянного виртуального канала (3 байта).
Control - поле управления (1 байт).
HCS - поле контрольной суммы (1 байт).
AL - поле адаптационного уровня АТМ (4 байта).

Как видно из таблицы, ячейка имеет размер 53 октета и включает заголовок длиной 5 октетов и информационное поле. Первые четыре двоичных символа заголовка выделены для поля общего управления потоком. Следующие 24 двоичных единицы используются для идентификации виртуального пути (ВП) и виртуального канала (ВК). Как отмечалось выше, сети АТМ являются ориентированными на соединение, и требуемая виртуальная цепь должна быть проложена через сеть АТМ прежде, чем какие-либо данные будут переданы. Для организации этой цепи технология АТМ предусматривает использование виртуальных каналов. Несколько ВК составляют виртуальный путь /14/. Все идентификаторы виртуальных путей и виртуальных каналов (ИВП и ИВК) имеют только местное значение в пределах отдельной линии и принимают новые значения в каждом коммутаторе сети АТМ. Ряд ИВК резервируется для трафика сигнализации и различных целей управления.

Три двоичных символа четвертого октета используются для идентификации типа сообщения, передаваемого в информационном поле ячейки (данные пользователя или служебная информация управления, контроля и обеспечения). Данное поле “тип полезной нагрузки” также может использоваться для информирования о перегрузке в сети.

В пятом октете заголовка содержится проверочная последовательность заголовка. Ячейка уничтожается, если в ее заголовке обнаруживается ошибка. Кроме того с помощью этого поля выполняется синхронизация ячеек АТМ. При отсутствии синхронизма по принятым четырем байтам вычисляется проверочный байт. Процедура повторяется до тех пор пока найденный таким образом проверочный байт не совпадет с принятым пятым байтом, после чего наличие синхронизации проверяется каждые 53 байта. Для поддержания синхронизации ячейки передаются постоянно, даже если нет информации для передачи. В этом случае посылаются пустые ячейки.

Формат ячейки, определенный для интерфейса NNI, немного отличается от рассмотренного. NNI-ячейки в отличие от ячеек UNI не содержат поля управления общим потоком, и четыре первых бита каждой ячейки используются расширенным полем идентификатора виртуального пути (12 бит). Поскольку поле управления общим потоком используется редко, но существует (его использование не определено, например, в решениях по UNI консорциума Форум АТМ), на практике функционального различия между ячейками UNI и NNI нет, кроме разве того, что ячейка последнего может поддерживать большее пространство идентификаторов ВП.

Сеть АТМ строится на основе соединенных друг с другом АТМ-коммутаторов. Технология реализуется как в локальных, так и в глобальных сетях. Допускается совместная передача различных видов информации, включая видео, голос.

Ячейки данных, используемые в АТМ, меньше в сравнении с элементами данных, которые используются в других технологиях. Небольшой, постоянный размер ячейки, используемый в АТМ, позволяет:

- Совместно передавать данные с различными классами требований к задержкам в сети, причём по каналам как с высокой, так и с низкой пропускной способностью;
- Работать с постоянными и переменными потоками данных;
- Интегрировать на одном канале любые виды информации: данные, голос, потоковое аудио- и видеовещание, телеметрия и т. п.;
- Поддерживать соединения типа точка–точка, точка–многоточка и многоточка–многоточка.

Технология АТМ предполагает межсетевое взаимодействие на трёх уровнях.

Для передачи данных от отправителя к получателю в сети АТМ создаются *виртуальные каналы*, VC (англ. *Virtual Circuit*), которые бывают трёх видов:

- *постоянный виртуальный канал*, PVC (Permanent Virtual Circuit), который создаётся между двумя точками и существует в течение длительного времени, даже в отсутствие данных для передачи;

- *коммутируемый виртуальный канал*, SVC (Switched Virtual Circuit), который создаётся между двумя точками непосредственно перед передачей данных и разрывается после окончания сеанса связи.
- *автоматически настраиваемый постоянный виртуальный канал*, SPVC (Soft Permanent Virtual Circuit). Каналы SPVC по сути представляют собой каналы PVC, которые инициализируются по требованию в коммутаторах ATM. С точки зрения каждого участника соединения, SPVC выглядит как обычный PVC, а что касается коммутаторов ATM в инфраструктуре провайдера, то для них каналы SPVC имеют значительные отличия от PVC. Канал PVC создаётся путём статического определения конфигурации в рамках всей инфраструктуры провайдера и всегда находится в состоянии готовности. Но в канале SPVC соединение является статическим только от конечной точки (устройство DTE) до первого коммутатора ATM (устройство DCE). А на участке от устройства DCE отправителя до устройства DCE получателя в пределах инфраструктуры провайдера соединение может формироваться, разрываться и снова устанавливаться по требованию. Установленное соединение продолжает оставаться статическим до тех пор, пока нарушение работы одного из звеньев канала не вызовет прекращения функционирования этого виртуального канала в пределах инфраструктуры провайдера сети.

Для маршрутизации в пакетах используют так называемые идентификаторы пакета. Они бывают двух видов:

- **VPI** (англ. *virtualpathidentifier*) — идентификатор виртуального пути (номер канала)
- **VCI** (англ. *virtualcircuitidentifier*) — идентификатор виртуального канала (номер соединения)

Сеть ATM - это набор коммутаторов и оконечных систем (хостов, маршрутизаторов и т.д.) ATM, связанных между собой межточечными каналами связи (point-to-point links), либо интерфейсами UNI или NNI. Первый тип интерфейса (UNI) используется при соединении оконечных систем ATM, второй (NNI) - при соединении коммутаторов ATM.

Задачи коммутатора ATM по сути очень просты: при известном значении ИВК или ИВП получить некоторую ячейку по каналу связи, найти соответствующее соединение в местной таблице преобразования, чтобы тем самым определить выходной порт (или порты), а также новые ВК и ВП для такого соединения на данном канале связи, после чего данная ячейка вместе с соответствующими идентификаторами передается на выходной канал связи.

Каждой передаче данных предшествует настройка местных таблиц преобразования, осуществляемая извне. По способу настройки таких таблиц различают два основных типа АТМ-соединения:

Постоянное виртуальное соединение (Permanent Virtual Connection, PVC). Соединение PVC устанавливается посредством какого-либо внешнего механизма, как правило, посредством административного управления сетью. При этом ряд коммутаторов между источником и приемником АТМ программируется определенным значением ИВК и ИВП.

Коммутируемое виртуальное соединение (Switched Virtual Connection, SVC). Соединение SVC устанавливается автоматически, посредством сигнального протокола. Соединение SVC не требует ручного вмешательства, необходимого для настройки PVC, и, поэтому, оно получило более широкое распространение. Протоколы высокого уровня, действующие в сетях АТМ, как правило, используют SVC.

Существуют, в зависимости от типа соединения (SVC или PVC), два основных варианта соединения АТМ:

Межточечное соединение (point-to-point), при котором две оконечные АТМ-системы соединяются между собой. Такое соединение может быть однонаправленным или двунаправленным.

Точечно-многоточечное соединение (point-to-multipoint), при котором одна передающая оконечная АТМ-система (так называемый “корневой узел”) соединяется с несколькими принимающими оконечными системами (их называют “концевыми узлами”). Тиражирование ячеек в сети осуществляется посредством коммутаторов АТМ, в которых соединение расходится на несколько ветвей. Такое соединение является однонаправленным и позволяет передавать информацию из корня на концевые узлы, в то время как концевые узлы, в рамках того же соединения, не могут передавать информацию корню или друг другу.

Необходимо отметить, что среди перечисленных вариантов АТМ-соединений отсутствуют возможности широковещательной (broadcasting) или групповой (многоадресной) передачи (multicasting), характерные для многих ЛВС среднего уровня с общей средой передачи данных, таких как Ethernet и Token Ring. В сетях АТМ аналогом групповой (многоадресной) передачи могло бы стать “многоточечно-многоточечное” соединение. Однако такое решение не реализуемо из-за того, что в наиболее распространенном 5 варианте уровня AAL (AAL5), который применяется для передачи данных в сетях АТМ, не предусмотрено никаких средств для чередования ячеек из разных пакетов в одном соединении. Это значит, что все пакеты AAL5, посланные по

определенному соединению и в определенном направлении, будут приняты последовательно, без чередования ячеек из различных пакетов, поскольку в противном случае приемник не сможет восстановить полученные пакеты.

Для решения задачи групповой (многоадресной) передачи в АТМ возможны три способа:

Групповая (многоадресная) передача по виртуальному пути. При таком механизме, все узлы группы многоадресной передачи соединяются между собой по многоточечно-многоточечному виртуальному пути, причем каждому узлу назначается свое собственное, уникальное значение ИВК, в рамках данного ВП. Таким образом, пакеты могут быть распознаны по уникальному значению ИВК источника.

Сервер групповой (многоадресной) передачи. При таком механизме все узлы, передающие данные в группу многоадресной передачи, устанавливают межточечную связь с внешним устройством, которое называется сервером групповой (многоадресной) передачи. Посредством точечно-многоточечной связи такой сервер, с свою очередь, присоединен ко всем узлам, принимающим пакеты групповой (многоадресной) передачи. Сервер получает пакеты по межточечным соединениям, а затем передает их через точечно-многоточечное соединение, но только после того, как убедится, что пакеты организованы в последовательности (то есть следующий пакет пересылается только по окончании пересылки предыдущего). Таким образом, предотвращается смешивание ячеек.

Оверлейные точечно-многоточечные соединения. При таком механизме, каждый узел группы многоадресной передачи устанавливает точечно-многоточечное соединение со всеми узлами группы и, в свою очередь, становится концевым узлом в равнозначных соединениях всех остальных узлов. Следовательно, все узлы могут как передавать сигналы на все остальные узлы, так и принимать их со всех остальных узлов.

1.13 Лекция №15 (2 часа).

Тема: «Сетевые операционные системы»

1.13.1 Вопросы лекции:

1. Структура сетевой ОС.
2. Сетевые ОС фирмы Microsoft.

1.13.2 Краткое содержание вопросов:

1. Структура сетевой операционной системы

Сетевая операционная система составляет основу любой вычислительной сети. Каждый компьютер в сети в значительной степени автономен, поэтому под сетевой операционной системой в широком смысле понимается совокупность операционных

систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам - протоколам. В узком смысле сетевая ОС - это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

К возможностям сетевых ОС относится поддержка следующего:

- сетевого оборудования;
- сетевых протоколов;
- протоколов маршрутизации;
- фильтрации сетевого трафика;
- доступа к удалённым ресурсам: принтерам, дискам посредством сети;
- сетевых протоколов авторизации.

Сетевая ОС также включает в себя сетевые службы, позволяющие удалённым пользователям использовать те или иные ресурсы компьютера.

Примеры сетевых операционных систем:

- Novell NetWare
- LANtastic
- Microsoft Windows (NT, XP, Vista, 7, 8, 8.1, 10)
- Различные UNIX системы, такие как Solaris, FreeBSD
- Различные GNU/Linux системы

Главными задачами сетевых ОС являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети. С помощью сетевых функций системный администратор определяет разделяемые ресурсы, задаёт пароли, определяет права доступа для каждого пользователя или группы пользователей. Отсюда деление:

- сетевые ОС для серверов;
- сетевые ОС для пользователей.

Существуют специальные сетевые ОС, которым приданы функции обычных систем (например, Windows NT) и обычные ОС (например, Windows XP), которым приданы сетевые функции. Сегодня практически все современные ОС имеют встроенные сетевые функции.

В сетевой операционной системе отдельной машины можно выделить несколько частей (рисунок 37):

Рисунок 37. Структура сетевой ОС

Средства управления локальными ресурсами компьютера: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами в мультипроцессорных машинах, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.

Средства предоставления собственных ресурсов и услуг в общее пользование - серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, что необходимо для их совместного использования; ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей ксвоим периферийным устройствам.

Средства запроса доступа к удаленным ресурсам и услугам и их использования - клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т.п., то есть является средством транспортировки сообщений.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

На рисунке 38 показано взаимодействие сетевых компонентов. Здесь компьютер 1 выполняет роль "чистого" клиента, а компьютер 2 - роль "чистого" сервера, соответственно на первой машине отсутствует серверная часть, а на второй - клиентская. На рисунке отдельно показан компонент клиентской части - редиректор. Именно редиректор перехватывает все запросы, поступающие от приложений, и анализирует их. Если выдан запрос к ресурсу данного компьютера, то он переадресовывается соответствующей подсистеме локальной ОС, если же это запрос к удаленному ресурсу, то он переправляется в сеть. При этом клиентская часть преобразует запрос из локальной формы в сетевой формат и передает его транспортной подсистеме, которая отвечает за доставку сообщений указанному серверу. Серверная часть операционной системы компьютера 2 принимает запрос, преобразует его и передает для выполнения своей локальной ОС. После того, как результат получен, сервер обращается к транспортной подсистеме и направляет ответ клиенту, выдавшему запрос. Клиентская часть преобразует результат в соответствующий формат и адресует его тому приложению, которое выдало запрос.

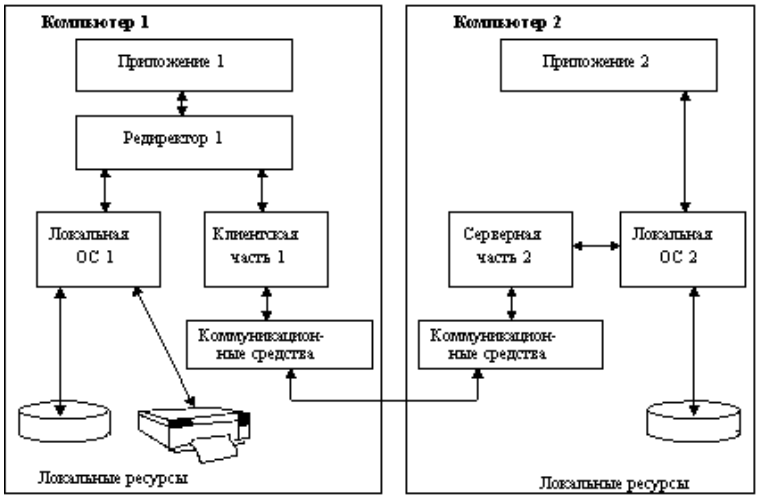


Рисунок 38. взаимодействие компонентов операционной системы при взаимодействии компьютеров

На практике сложилось несколько подходов к построению сетевых операционных систем (рисунок 39).

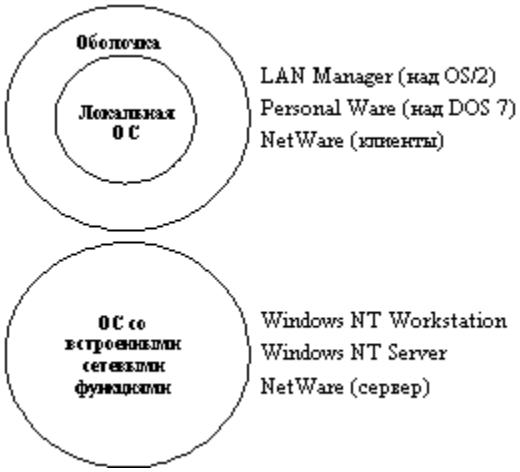


Рисунок 39. Варианты построения сетевых ОС

Первые сетевые ОС представляли собой совокупность существующей локальной ОС и надстроенной над ней сетевой оболочки. При этом в локальную ОС встраивался минимум сетевых функций, необходимых для работы сетевой оболочки, которая выполняла основные сетевые функции. Примером такого подхода является использование на каждой машине сети операционной системы MS DOS (у которой начиная с ее третьей версии появились такие встроенные функции, как блокировка файлов и записей, необходимые для совместного доступа к файлам). Принцип построения сетевых ОС в виде сетевой оболочки над локальной ОС используется и в современных ОС, таких, например, как LANtastic или Personal Ware.

Однако более эффективным представляется путь разработки операционных систем, изначально предназначенных для работы в сети. Сетевые функции у ОС такого типа глубоко встроены в основные модули системы, что обеспечивает их логическую стройность, простоту эксплуатации и модификации, а также высокую производительность. Примером такой ОС является система Windows NT фирмы Microsoft, которая за счет встроенности сетевых средств обеспечивает более высокие показатели производительности и защищенности информации по сравнению с сетевой ОС LAN Manager той же фирмы (совместная разработка с IBM), являющейся надстройкой над локальной операционной системой OS/2.

2. Сетевые ОС фирмы Microsoft.

В 1984 году Microsoft выпустила свой первый сетевой продукт, называемый Microsoft Networks, который обычно неформально называют MS-NET. Некоторые концепции, заложенные в MS-NET, такие как введение в структуру базовых компонент -

редиректора и сетевого сервера - успешно перешли в LAN Manager, а затем и в Windows NT.

Microsoft все еще поставляет свою сетевую ОС LAN Manager. Большое количество независимых поставщиков имеют лицензии на эту ОС и поддерживают свои собственные версии LAN Manager как часть своих сетевых продуктов. В число этих компаний входят такие известные фирмы как AT&T и Hewlett-Packard. LAN Manager требует установки на файл-сервере операционной системы OS/2, рабочие станции могут работать под DOS, Windows или OS/2. OS/2 - это операционная система, реализующая истинную многозадачность, работающая в защищенном режиме микропроцессоров x86 и выше. LAN Manager использует 32-х битную версию файловой системы OS/2, называемую HPFS, которая оптимизирована для работы на файл-сервере за счет кэширования каталогов и данных. LAN Manager - это первая сетевая ОС, разработанная для поддержки среды клиент-сервер. Ключевыми компонентами LAN Manager являются редиректор и сервер. Особенно эффективно LAN Manager поддерживает архитектуру клиент-сервер для систем управления базами данных. LAN Manager разрешает рабочим станциям под OS/2 поддерживать сетевой сервис по технологии "равный-с-равным". Это означает, что рабочая станция может выполнять функции сервера баз данных, принт-сервера или коммуникационного сервера. Ограничением является то, что только один пользователь, кроме владельца этой рабочей станции, имеет доступ к такому одноранговому сервису.

Для работы в небольшой сети фирма Microsoft предлагает компактную, не требующую значительных аппаратных или программных затрат операционную систему Windows for Workgroups. Эта операционная система позволяет организовать сеть по схеме "равный-с-равным", при этом нет необходимости приобретать специальный компьютер для работы в качестве сетевого сервера. Эта операционная система особенно подходит для решения сетевых задач в коллективах, члены которого ранее широко использовали Windows 3.1. В Windows for Workgroups достигнута высокая производительность сетевой обработки за счет того, что все сетевые драйверы являются 32-х разрядными виртуальными драйверами.

С середины 1993 года Microsoft начала выпуск новых операционных систем "новой технологии" (New Technology - NT) Windows NT.

В сентябре 1995 года компания Microsoft выпустила еще одну новую операционную систему Windows 95 (кодовое название Chicago), предназначенную для замены Windows 3.1 и Windows for Workgroups 3.11 в настольных компьютерах с процессорами Intel x86.

В 1995-м году фирмой Microsoft была разработана операционная система Windows NT в качестве серверной платформы. Windows NT является уникальной и мощной ОС. При ее разработке преследовались следующие цели: надежность, производительность, переносимость, масштабируемость, совместимость и безопасность.

Надежность позволяет использовать Windows NT в качестве основы для задач, требующих именно этого свойства. Она идеально приспособлена для работы в качестве сетевого сервера и рабочей станции, где требуется повышенная устойчивость и высокая производительность.

Будучи истинно 32-х разрядной системой, Windows NT работает в 32-х битовой линейной модели памяти, которая позволяет адресовать 4 Гбайт (свыше 4-х миллиардов байт) памяти.

Windows NT использует метод вытесняющей многозадачности, что гарантирует адекватное распределение ресурсов процессора на протяжении всей работы системы. Это также предотвращает монопольный захват процессора приложением и остановку системы в тех случаях, когда приложение работает нестабильно или внезапно прекратило работу. Это позволяет Windows NT работать даже тогда, когда другая операционная система окончательно бы зависла.

Транзакционная файловая система (NTFS) Windows NT усовершенствована и предельно надежна. Используя транзакции, Windows NT имеет возможность отменить незавершенную или неправильную операцию записи, возникающую в случае сбоя аппаратного или программного обеспечения (например, внезапное отключение электропитания во время записи файла). Благодаря такому подходу файловая система Windows NT гораздо менее подвержена разрушению при различных нештатных ситуациях.

Все составляющие части Windows NT используют 32-х битовый код что позволяет повысить скорость работы по сравнению операционными системами использующими 16-ти разрядную технологию.

Операционная система Windows NT существует в двух вариантах - Wndows NT Server и Windows NT Workstation. Первая предназначена для использования в качестве сервера и имеет все возможности для его реализации. Вторая предназначена для рабочих станций, ее целесообразно использовать на рабочих станциях, где требуется повышенная защищенность и надежность работы.

На текущий момент фирмой Microsoft выпущена ОС Windows 2000. В эту версию вложено несколько новых усовершенствований, среди них: поддержка файловой системы FAT32, в связи с чем стало возможным использование жестких дисков больших емкостей

и возможность использование их емкости с меньшими потерями, по сравнению с более старой файловой системой FAT16. Еще в систему внесена технология Plug-and-Play, позволяющая упростить процесс инсталляции новых аппаратных компонентов. В операционной системе Windows NT этих возможностей не было.

Эта система также выпущена в двух вариантах Windows 2000 Server - для сервера и Windows 2000 Professional - для рабочих станций. В недалеком будущем фирма Microsoft планирует выпуск новых сетевых операционных систем.

1.14. Лекция №16 (2 часа).

Тема: Технология TokenRing.

1.14.1 Вопросы лекции:

1. Оборудование TR.
2. Топология TR.

1.14.2 Краткое содержание вопросов:

1. Оборудование TR.

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

Технология Token Ring был разработана компанией IBM в 1984 году, а затем передана в качестве проекта стандарта в комитет IEEE 802, который на ее основе принял в 1985 году стандарт 802.5. Компания IBM использует технологию Token Ring в качестве своей основной сетевой технологии для построения локальных сетей на основе компьютеров различных классов - мэйнфреймов, мини-компьютеров и персональных компьютеров. В настоящее время именно компания IBM является основным законодателем моды технологии Token Ring, производя около 60 % сетевых адаптеров этой технологии.

Сети Token Ring работают с двумя битовыми скоростями - 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается. Сети Token Ring, работающие со скоростью 16 Мбит/с, имеют некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мбит/с.

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры - посланный кадр всегда возвращается в станцию - отправитель. В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

Для контроля сети одна из станций выполняет роль так называемого *активного монитора*. Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC-адреса, Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Чтобы сеть могла обнаружить отказ активного монитора, последний в работоспособном состоянии каждые 3 секунды генерирует специальный кадр своего присутствия. Если этот кадр не появляется в сети более 7 секунд, то остальные станции сети начинают процедуру выборов нового активного монитора.

Оборудование TR.

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

Конструктивно концентратор представляет собой автономный блок с десятью разъемами на передней панели (рис. 40).

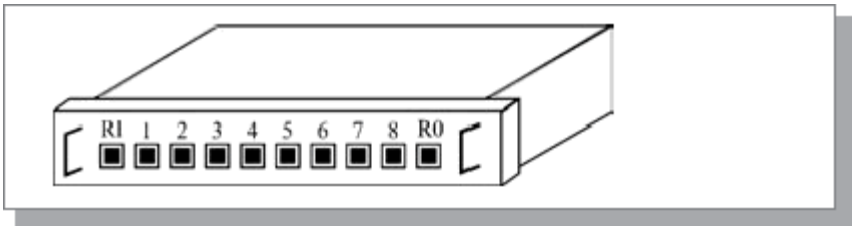


Рисунок 40. Концентратор Token-Ring (8228 MAU)

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

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

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

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

2. Топология TR.

Сеть ***Token-Ring*** имеет топологию кольцо, хотя внешне она больше напоминает звезду. Это связано с тем, что отдельные абоненты (компьютеры) присоединяются к сети не напрямую, а через специальные концентраторы или многостанционные устройства доступа (*MSAU*или *MAU* – Multistation *Access Unit*). Физически сеть образует звездно-кольцевую топологию (рисунок 41). В действительности же абоненты объединяются все-таки в кольцо, то есть каждый из них передает информацию одному соседнему абоненту, а принимает информацию от другого.

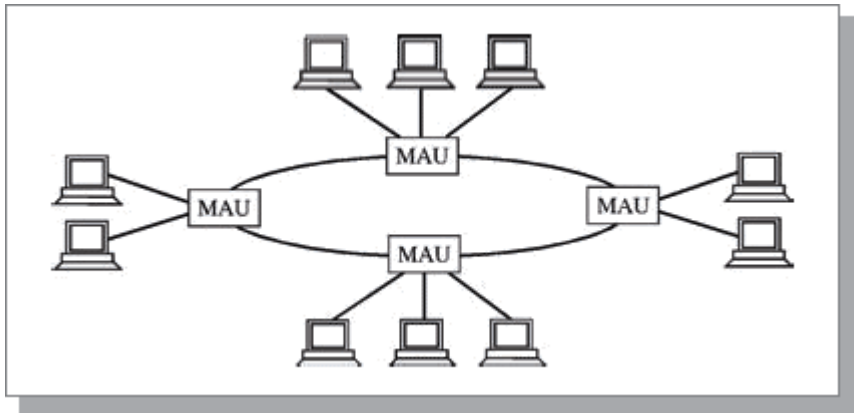


Рисунок 41. Звездно-кольцевая топология сети Token-Ring

Концентратор (*MAU*) при этом позволяет централизовать задание конфигурации, отключение неисправных абонентов, *контроль* работы сети и т.д. Никакой обработки информации он не производит.

Для каждого абонента в составе концентратора применяется специальный блок подключения к магистрали (TCU – *Trunk Coupling* Unit), который обеспечивает автоматическое включение абонента в кольцо, если он подключен к концентратору и исправен. Если *абонент*отключается от концентратора или же он неисправен, то блок TCU автоматически восстанавливает *целостность* кольца без участия данного абонента. Срабатывает TCU *по* сигналу постоянного тока (так называемый "фантомный" ток), который приходит от абонента, желающего включиться в кольцо. *Абонент* может также отключиться от кольца и провести процедуру *самотестирования*. "Фантомный" ток никак не влияет на информационный сигнал, так как сигнал в кольце не имеет постоянной составляющей.

Эта топология основана на топологии "физическое кольцо с подключением типа звезда". В данной топологии все рабочие станции подключаются к центральному концентратору (TokenRing) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое с помощью перемычек обеспечивает последовательное соединение выхода одной станции со входом другой станции.

Другими словами с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой и каждая станция ретранслирует эти посланные пакеты. В каждой рабочей станции имеется для этого приемо-передающее устройство, которое позволяет

управлять прохождением данных в сети. Физически такая сеть построена по типу топологии “звезда”.

Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не вличет за собой отказ сети как в топологии кольцо, потому что концентратор отключет неисправную станцию и замкнет кольцо передачи данных.

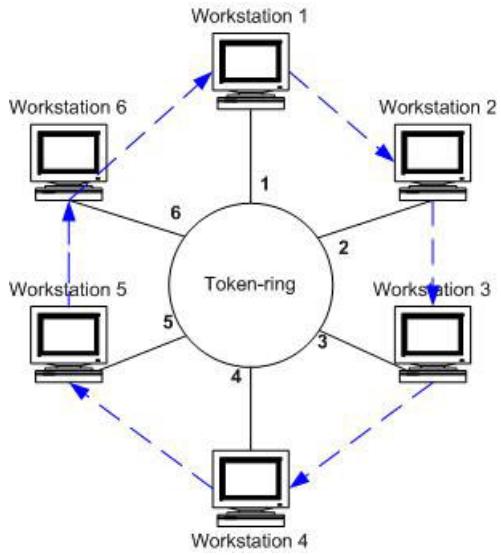


Рисунок 42 - Топология TokenRing

В архитектуре TokenRing маркер передаётся от узла к узлу по логическому кольцу, созданному центральным концентратором. Такая маркерная передача осуществляется в фиксированном направлении (направление движения маркера и пакетов данных представлено на рисунке стрелками синего цвета). Станция, обладающая маркером, может отправить данные другой станции.

Для передачи данных рабочие станции должны сначала дождаться прихода свободного маркера. В маркере содержится адрес станции, пославшей этот маркер, а также адрес той станции, которой он предназначается. После этого отправитель передает маркер следующей в сети станции для того, чтобы и та могла отправить свои данные.

Один из узлов сети (обычно для этого используется файл-сервер) создаёт маркер, который отправляется в кольцо сети. Такой узел выступает в качестве активного монитора, который следит за тем, чтобы маркер не был утерян или разрушен.

Основные *технические характеристики* классического варианта сети *Token-Ring*:

- максимальное количество концентраторов типа IBM 8228 *MAU* – 12;

- максимальное количество абонентов в сети – 96;
- максимальная длина кабеля между абонентом и концентратором – 45 метров;
- максимальная длина кабеля между концентраторами – 45 метров;
- максимальная длина кабеля, соединяющего все концентраторы – 120 метров;
- скорость передачи данных – 4 Мбит/с и 16 Мбит/с.

Все приведенные характеристики относятся к случаю использования неэкранированной витой пары. Если применяется другая *среда передачи*, характеристики сети могут отличаться. Например, при использовании экранированной витой пары (*STP*) количество абонентов может быть увеличено до 260 (вместо 96), *длина* кабеля – до 100 метров (вместо 45), количество концентраторов – до 33, а полная *длина*кольца, соединяющего *концентраторы* – до 200 метров. Оптоволоконный *кабель* позволяет увеличивать длину кабеля до двух километров.

Преимущества сетей топологии TokenRing:

- топология обеспечивает равный доступ ко всем рабочим станциям;

- высокая надежность, так как сеть устойчива к неисправностям отдельных станций и к разрывам соединения отдельных станций.

Недостатки сетей топологии TokenRing: большой расход кабеля и соответственно дорогостоящая разводка линий связи.

1.15 Лекция №17 (2 часа).

Тема: «Технология Frame Relay»

Вопросы лекции:

1. Технология FrameRealy

1. Технология FrameRealy

Сеть Frame Relay является сетью с коммутацией кадров или сетью с ретрансляцией кадров, ориентированной на использование цифровых линий связи. Первоначально технология Frame Relay была стандартизирована как служба в сетях ISDN со скоростью передачи данных до 2 Мбит/с. В дальнейшем эта технология получила самостоятельное развитие. Frame Relay поддерживает физический и канальный уровни OSI. Технология Frame Relay использует для передачи данных технику виртуальных соединений (коммутируемых и постоянных).

Стек протоколов Frame Relay передает кадры при установленном виртуальном соединении по протоколам физического и канального уровней. В Frame Relay функции сетевого уровня перемещены на канальный уровень, поэтому необходимость в сетевом

уровне отпала. На канальном уровне в Frame Relay выполняется мультиплексирование потока данных в кадры.

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

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

Сети Frame Relay широко используется в корпоративных и территориальных сетях в качестве:

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

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

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

Рисунок 43. Сеть Frame Relay

На рисунке представлена структурная схема сети Frame Relay, где изображены основные элементы:

1. DTE (data terminal equipment) – аппаратура передачи данных (маршрутизаторы, мосты, ПК).

2. DCE (data circuit-terminating equipment) – оконечное оборудование канала передачи данных (телекоммуникационное оборудование, обеспечивающее доступ к сети).

Физический уровень Frame Relay

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

Канальный уровень Frame Relay

В сети Frame Relay используется два типа виртуальных каналов: постоянные (PVC) и коммутируемые виртуальные каналы. На канальном уровне поток данных структурируется на кадры, поле данных в кадре имеет переменную величину, но не более 4096 байт. Канальный уровень реализуется протоколом LAP-F. Протокол LAP-F имеет два режима работы: основной и управляющий. В основном режиме кадры передаются без преобразования и контроля.

В поле заголовка кадра имеется информация, которая используется для управления виртуальным соединением в процессе передачи данных. Виртуальному соединению присваивается определенный номер (DLCI). DLCI (Data Link Connection Identifier) - идентификатор соединения канала данных.

Каждый кадр канального уровня содержит номер логического соединения, который используется для маршрутизации и коммутации трафика. При этом контроль правильности передачи данных от отправителя получателю осуществляется на более высоком уровне модели OSI.

Коммутируемые виртуальные каналы используются для передачи импульсного трафика между двумя устройствами DTE. Постоянные виртуальные каналы применяются для постоянного обмена сообщениями между двумя устройствами DTE.

Процесс передачи данных через коммутируемые виртуальные каналы осуществляется следующим образом:

- установление вызова - образуется коммутируемый логический канал между двумя DTE;
- передача данных по установленному логическому каналу;
- режим ожидания, когда коммутируемая виртуальная цепь установлена, но обмен данными не происходит;
- завершение вызова - используется для завершения сеанса, осуществляется разрыв конкретного виртуального соединения.

Процесс передачи данных через предварительно установленные постоянные виртуальные каналы осуществляется следующим образом:

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

Протокол FR – это интерфейс доступа к сетям быстрой коммутации пакетов. Он позволяет эффективно передавать крайне неравномерно распределенный во времени трафик. Отличительные особенности протокола FR: малое время задержки при передаче информации через сеть, высокие скорости передачи, «высокая степень связности», эффективное использование полосы пропускания. По сетям FR возможна передача не только собственно данных, но и оцифрованного голоса.

Протокол FR выполняет функции первого, частично второго и третьего уровней модели ВОС. Он позволяет устанавливать соединение между взаимодействующими узлами сети, что аналогично соединению по X.25 в случае, когда используется постоянное виртуальное соединение (PVC). Внутри каждого физического канала может быть создана совокупность PVC (логических каналов), что и объясняет «высокую степень связности», обеспечиваемую протоколом FR. Что касается коммутируемых виртуальных соединений (SVC), то их использование в FR-сетях описывается специальными протоколами.

В отличие от сетей X.25, где на сетевом уровне обеспечивается гарантированная передача пакетов (в случае искажения при передаче какого-либо пакета происходит его повторная передача), кадр FR не содержит переменных нумераций передаваемых и подтверждаемых кадров. При межузловом обмене информацией в сетях FR ошибочные

кадры просто «выбрасываются», их повторная передача средствами FR не происходит. Для обеспечения гарантированной и упорядоченной передачи кадров необходимо использовать либо протоколы более высокого уровня (например, протокол TCP/IP), либо дополнение к протоколу FR (например, Q.922).

Кадр FR-сети имеет минимальную избыточность, т.е. доля служебной информации в кадре по отношению к передаваемым данным пользователя минимальна. Это способствует сокращению времени на передачу фиксированного объема информации. Кроме того, в сети FR может производиться маршрутизация своими средствами (беззадействования механизмов маршрутизации по X.25 или по протоколу IP), что значительно увеличивает скорость маршрутизации. Однако такой эффект достигается только при использовании каналов, качество которых соответствует требованиям технологии FR. В противном случае сравнительно много кадров будут передаваться с ошибкой, и потребуется повторная передача кадров, обеспечиваемая дополнительными средствами. Это снизит информационную скорость передачи информации и более эффективной в этом случае станет сеть X.25.

Эффективность технологии FR достигается также использованием специфических механизмов, управляющих загрузкой сети. Эти механизмы обеспечивают практически гарантированное время доставки кадров через сеть и одновременно дают возможность сети адаптироваться к крайне неравномерным во времени типам трафика (например, к трафику ЛКС).

Стремительному развитию технологии FR и повышению ее эффективности способствует ряд факторов, в частности улучшение качества каналов связи, использование современного многофункционального каналообразующего оборудования. К новому классу такого оборудования относятся мультимедийные пакетные коммутаторы (МПК).

Коммутаторы МПК, использующие технологию FR для транспортировки информации, совмещают несколько функций:

- статистическое уплотнение каналов передачи данных, при котором фиксированные промежутки времени в уплотняемом канале не предоставляются отдельно каждому каналу, как это имеет место при использовании метода временного уплотнения; информация каждого канала разбивается на отдельные блоки, к блоку прибавляются заголовок, содержащий идентификатор соответствующего канала, и хвост, что образует единицу передачи информации – кадр, с помощью которого могут передаваться все виды трафика. Основные преимущества такого уплотнения: динамическое распределение пропускной способности уплотненного канала связи в зависимости от активности в

каналах передачи данных, возможность предоставления пропускной способности по требованию, возможность установки приоритетов для различных видов трафика;

- коммутациию и передачу различных видов трафика;

- управление потоком информации и установка приоритетов;

- поддержку функций телефонных станций. К функциям АТС, выполняемым МПК, относятся оцифровка и коммутация голоса, передача факсимильных сообщений. Для технологии FR характерным является возможное увеличение задержки при передаче голоса по сравнению с обычной телефонной сетью. Устранить это явление можно путем установления более высокого приоритета для голосового трафика и применения фрагментации кадров.

Распространению технологии FR способствует также наличие стандартов, обеспечивающих совместимость сетей FR с другими сетями. Например, имеется стандарт IETF 1294 для преобразования пакетов TCP/IP в кадры FR. Есть стандарты, обеспечивающие совместимость FR с самыми высокопроизводительными и современными сетями – сетями ATM. При «входе» в сеть ATM длинные кадры FR разбиваются на короткие, размещаемые внутри ATM-ячеек, а при «выходе» из сети ATM из ячеек ATM-сети извлекаются фрагменты кадров FR и из них собираются полные кадры FR.

В настоящее время за рубежом, особенно в США, наблюдается стремительное развитие сетей FR. За один 1996 год число пользователей этих сетей выросло более чем в три раза. В начале 1997 г. около 1800 фирм США строили свои корпоративные сети на базе магистральных сетей FR. Наиболее распространенные способы доступа к сетям FR: использование выделенных линий; через сети X.25 по обычным коммутируемым телефонным линиям; через ISDN для передачи данных и голоса.

В России большинство сетей передачи данных общего пользования также предоставляют пользователям FR-сервис. Основная проблема с реализацией магистральной сети FR заключается в том, что те магистральные междугородние каналы, которые построены на базе телефонных линий (линий тональной частоты), не обеспечивают необходимое для сети FR качество передачи. Для построения сетей FR самые широкие возможности имеют те предприятия, решения которых основаны на базе оптоволоконных или спутниковых каналов связи.

Достоинства сети Frame Relay:

▪ высокая надежность работы сети;

▪ обеспечивает передачу чувствительный к временным задержкам трафик (голос, видеоизображение).

Недостатки сети Frame Relay:

- высокая стоимость качественных каналов связи;
- не обеспечивается достоверность доставки кадров.

Технология FR и в будущем сохранит свои преимущества и актуальность, поскольку она обеспечивает идеальный доступ к высокоскоростной магистральной ATM-сети по низкоскоростным каналам связи. Эта технология в настоящее время является наиболее эффективной для приложений, связанных с интеграцией неравномерного (пульсирующего) трафика локальных сетей, и чувствительной к задержке голосовой информации.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

2.1 Лабораторная работа № 1 (2 часа)

Тема: «Определение класса сети и выбор топологии»

2.1.1 Цель работы: ознакомится с вычислительными сетями, классификацией сетей. Приобрести навыки проектирования локальной вычислительной сети для конкретной организации с использованием различного типа оборудования. Научиться работать с локальными вычислительными сетям, кабельной системой, оборудованием (серверами, концентраторами, сетевыми адаптерами), использовать различные топологии локальных сетей.

2.1.2 Задачи работы:

1. Спроектировать ЛВС для организации, располагающейся в здании, состоящего из различного количества этажей и комнат на этажах;

2. При проектировании учитывать различные типы топологий (шина, звезда, кольцо);

3. Использовать различные типы сред передачи данных: сетевые кабели (коаскиальный кабель, витая пара проводов, оптоволокно), провода, радиоканалы наземной и спутниковой связи и т.д.

2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.1.4 Описание (ход) работы:

*Вычислительной сетью*называется система, состоящая из двух или более удаленных ЭВМ, соединенных с помощью специальной аппаратуры и взаимодействующих между собой по каналам передачи данных.

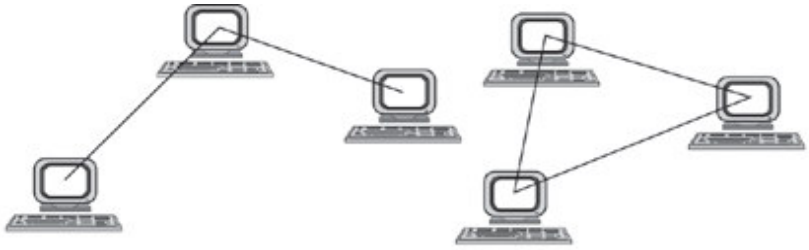
Самая простая сеть (network) состоит из нескольких персональных компьютеров, соединенных между собой сетевым кабелем. При этом в каждом компьютере устанавливается специальная плата сетевого адаптера (NIC), осуществляющая связь между системной шиной компьютера и сетевым кабелем.

Кроме этого, все компьютерные сети работают под управлением специальной сетевой операционной системы (NOS – Network Operation System). Основное назначение компьютерных сетей – совместное использование ресурсов и осуществление интерактивной связи как внутри одной фирмы, так и за ее пределами.

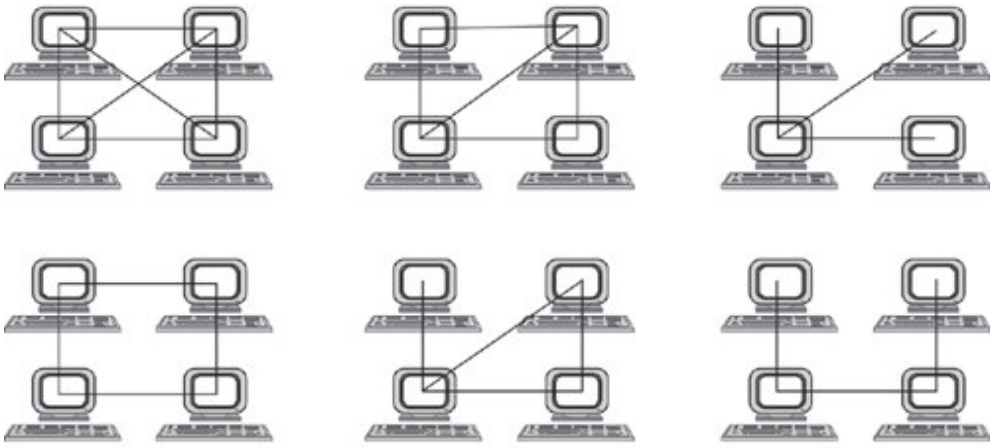
Как только компьютеров становится больше двух, возникает проблема выбора **конфигурации физических связей** или **топологии**. Под топологией сети понимается конфигурация графа, вершинам которого соответствуют конечные узлы сети (например, компьютеры) и коммуникационное оборудование (например, маршрутизаторы), а ребрам — электрические и информационные связи между ними.

Число возможных конфигураций резко возрастает при увеличении числа связываемых устройств. Так, если три компьютера мы можем связать двумя способами, то для четырех компьютеров (рисунок 1) можно предложить уже шесть топологически различных конфигураций (при условии неразличимости компьютеров).

Мы можем соединять каждый компьютер с каждым или же связывать их последовательно, предполагая, что они будут общаться, передавая друг другу сообщения "транзитом". При этом транзитные узлы должны быть оснащены специальными средствами, позволяющими выполнять эту специфическую посредническую операцию. В роли транзитного узла может выступать как универсальный компьютер, так и специализированное устройство.



а) вариант связи трех компьютеров



б) вариант связи четырех компьютеров

Рисунок 1 - Варианты связи компьютеров

От выбора топологии связей зависят многие характеристики сети. Например, наличие меду узлами нескольких путей повышает надежность сети и делает возможной балансировку загрузки отдельных каналов. Простота присоединения новых узлов, свойственная некоторым топологиям, делает сеть легко расширяемой. Экономические соображения часто приводят к выбору топологий, для которых характерна минимальная суммарная длина линий связи.

Среди множества возможных конфигураций различают **полносвязные** и **неполносвязные**:

Полносвязная топология (рисунок 2) соответствует сети, в которой каждый компьютер непосредственно связан со всеми остальными. Несмотря на логическую простоту, это вариант громоздкий и неэффективный. Действительно, каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров. Для каждой пары компьютеров должна быть выделена отдельная физическая линия связи (в некоторых случаях даже 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 связи, т.е. имеет место квадратическая зависимость. Чаще этот вид топологии используется в многомашинных комплексах или в сетях, объединяющих небольшое количество компьютеров.

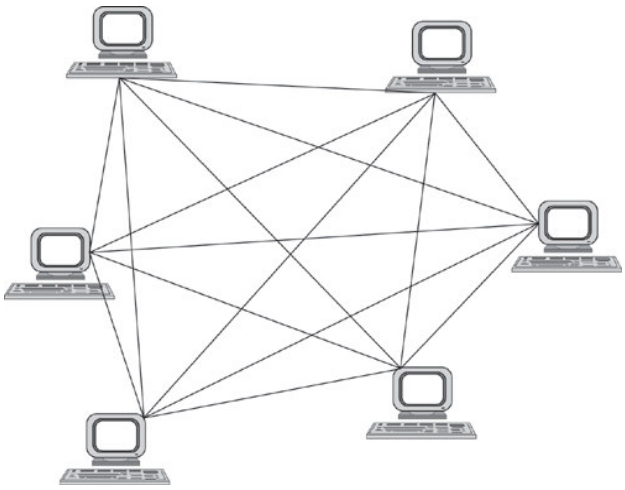


Рисунок 2 - Полносвязная конфигурация

Все другие варианты основаны на неполносвязных топологиях, когда для обмена данными между двумя компьютерами может потребоваться промежуточная передача данных через другие узлы сети.

Ячеистая топология получается из полносвязной путем удаления некоторых возможных связей. Ячеистая топология допускает соединение большого количества компьютеров и характерна для крупных сетей (рисунок 3).

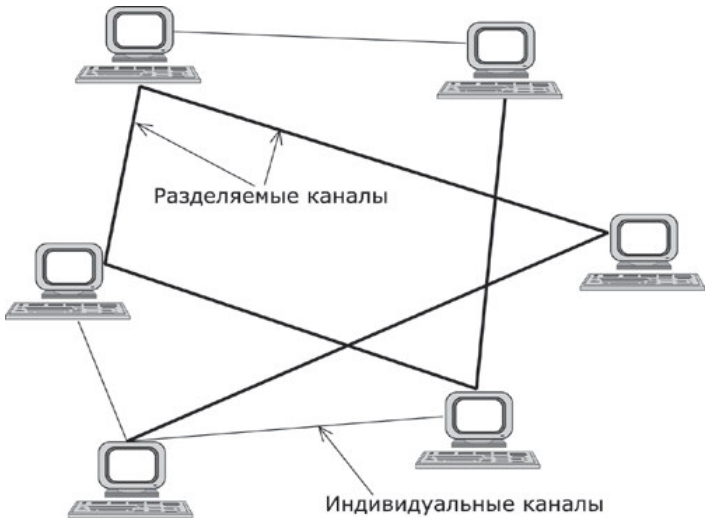


Рисунок 3 - Ячеистая топология

В сетях с кольцевой конфигурацией (рисунок 4) данные передаются по кольцу от одного компьютера к другому. Главное достоинство "кольца" в том, что оно по своей природе обладает свойством резервирования связей.

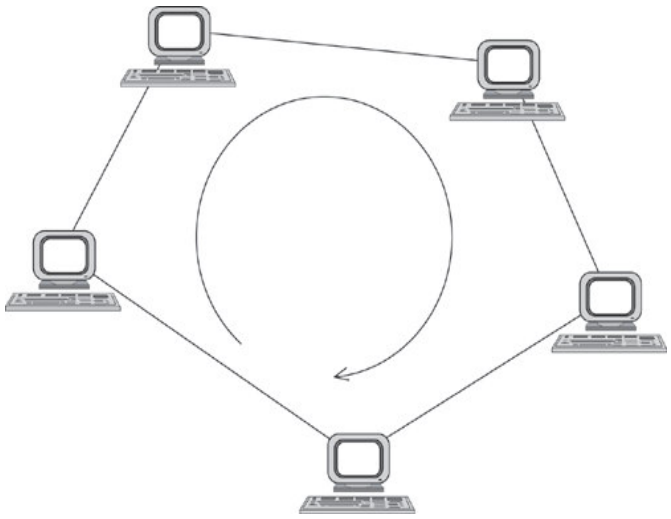


Рисунок 4 -Топология "кольцо"

Действительно, любая пара узлов соединена здесь двумя путями — по часовой стрелке и против. "Кольцо" представляет собой очень удобную конфигурацию и для организации обратной связи — данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому отправитель в данном случае может контролировать процесс доставки данных адресату. Часто это свойство "кольца" используется для тестирования связности сети и поиска узла, работающего некорректно. В то же время в сетях с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какой-либо станции не прерывался канал связи между остальными станциями "кольца".

Топология "звезда" (рисунок 5) образуется в том случае, когда каждый компьютер с помощью отдельного кабеля подключается к общему центральному устройству, называемому концентратором.

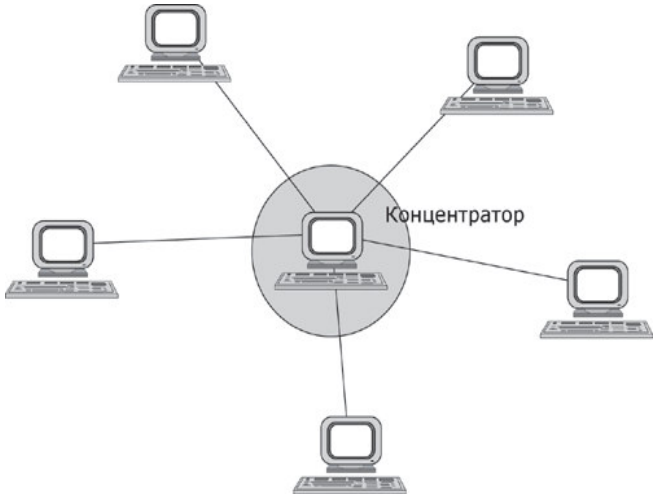


Рисунок 5 - Топология "звезда"

В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. В роли концентратора может выступать как компьютер, так и специализированное устройство, такое как многопортовый повторитель, коммутатор или маршрутизатор. К недостаткам топологии типа "звезда" относится более высокая стоимость сетевого оборудования, связанная с необходимостью приобретения специализированного центрального устройства. Кроме того, возможности наращивания количества узлов в сети ограничиваются количеством портов концентратора.

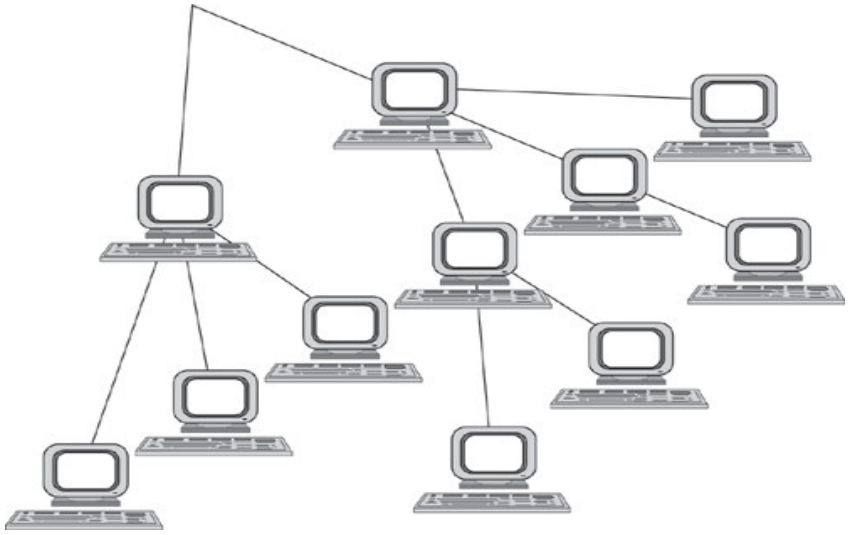


Рисунок 6 - Топология "иерархическая звезда" или "дерево"

Иногда имеет смысл строить сеть с использованием нескольких концентраторов, иерархически соединенных между собой связями типа "звезда" (рисунок 6).

Получаемую в результате **структуру** называют также деревом. В настоящее время дерево является самым распространенным типом топологии связей, как в локальных, так и в глобальных сетях.

Особым частным случаем конфигурации, звезда является конфигурация "общая шина" (рисунок 7).

Здесь в роли центрального элемента выступает пассивный кабель, к которому по схеме "монтажного ИЛИ" подключается несколько компьютеров (такую же топологию имеют многие сети, использующие беспроводную связь — роль общей шины здесь играет общая радиосреда).

Передаваемая информация распространяется по кабелю и доступна одновременно всем присоединенным к нему компьютерам.

Рисунок 7 - Топология "общая шина"

Основными преимуществами такой схемы являются низкая стоимость и простота наращивания, то есть присоединения новых узлов к сети.

Самым серьезным недостатком "общей шины" является ее недостаточная надежность: любой дефект кабеля или какого-нибудь из многочисленных разъемов полностью парализует всю сеть.

Другой недостаток "общей шины" — невысокая производительность, так как при таком способе подключения в каждый момент времени только один компьютер может передавать данные по сети, поэтому пропускная способность канала связи всегда делится между всеми узлами сети. До недавнего времени "общая шина" являлась одной из самых популярных топологий для локальных сетей.

В то время как небольшие сети, как правило, имеют типовую топологию — **"звезда"**, **"кольцо"** или **"общая шина"**, для крупных сетей характерно наличие произвольных связей между компьютерами.

В таких сетях можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовую топологию, поэтому их называют сетями со **смешанной** топологией (рисунок 8).

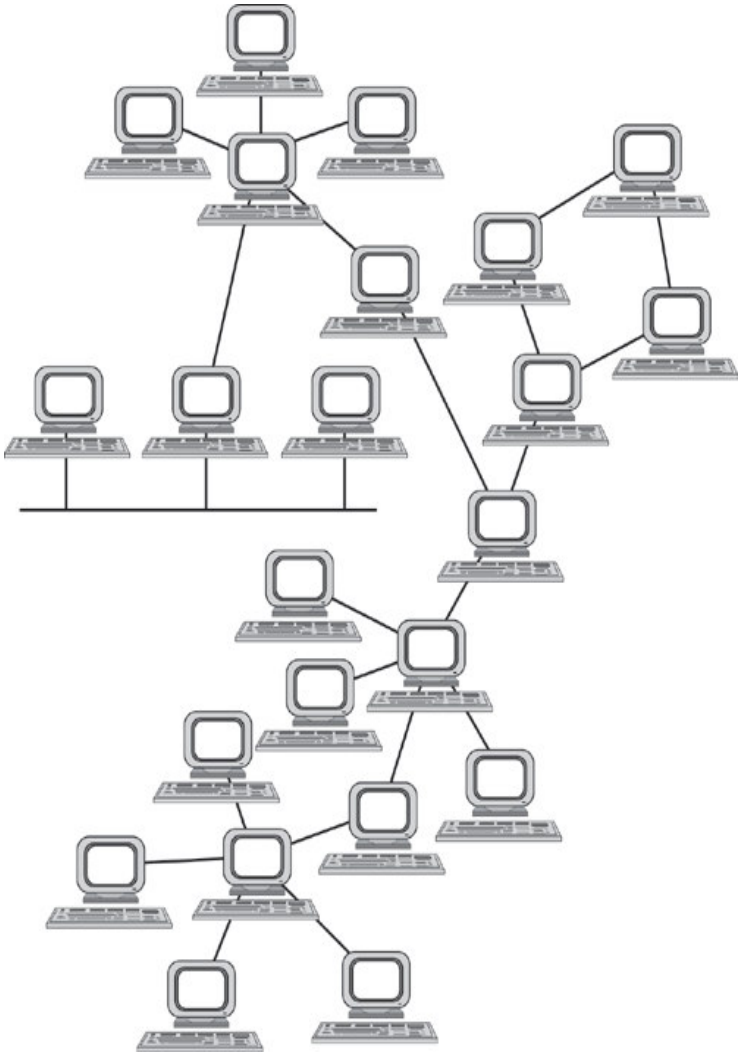


Рисунок 8 - Смешанная топология

Линия связи (рисунок 9) состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры. Синонимом термина *линия связи (line)* является термин *канал связи (channel)*.

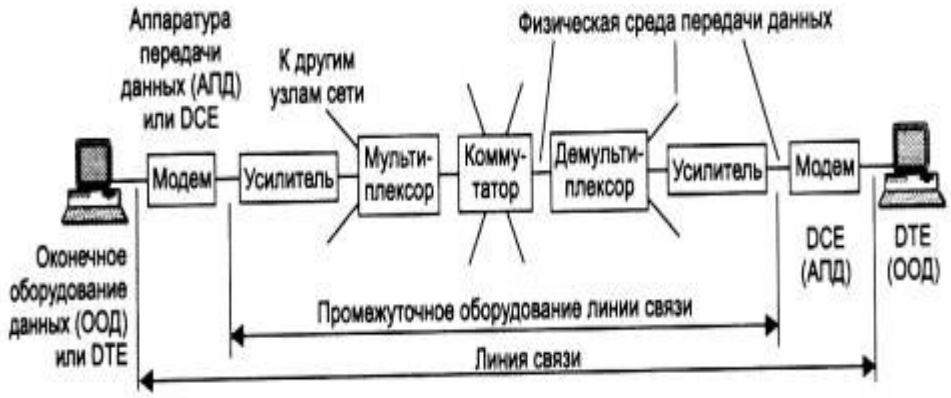


Рисунок 9 – Линии связи

Физическая среда передачи данных (medium) может представлять собой кабель, то есть набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В зависимости от среды передачи данных линии связи разделяются на следующие: проводные (воздушные), кабельные (медные и волоконно-оптические), радиоканалы наземной и спутниковой связи (рисунок 10):

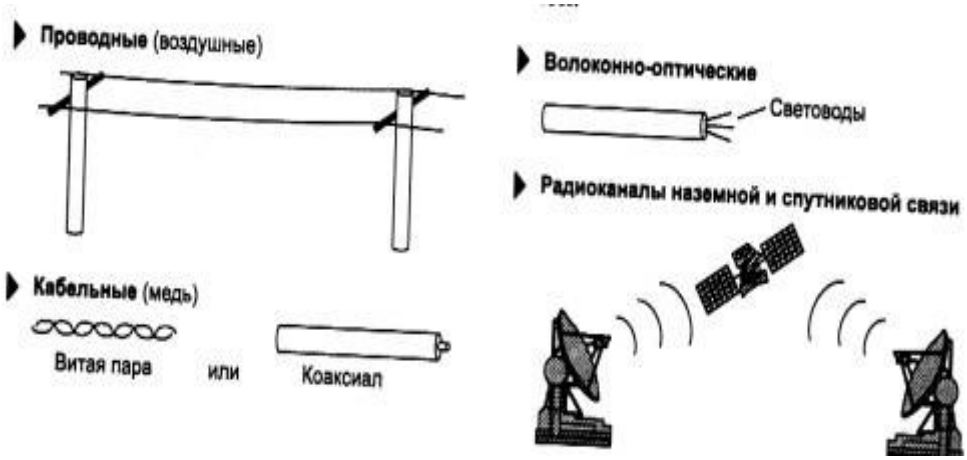


Рисунок 10 – Типы линий связи

Проводные (воздушные) линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи быстро вытесняются кабельными.

Кабельные линии представляют собой достаточно сложную конструкцию. Кабель состоит из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической, а также, возможно, климатической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных сетях применяются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой, а также волоконно-оптические кабели.

Скрученная пара проводов называется *витой парой (twisted pair)*. Витая пара существует в экранированном варианте *(Shielded Twistedpair, STP),* когда пара медных проводов обертывается в изоляционный экран, и неэкранированном *(Unshielded Twistedpair, UTP)*, когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

Коаксиальный кабель (coaxial) имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения - для локальных сетей, для глобальных сетей, для кабельного телевидения и т. п.

Волоконно-оптический кабель (optical fiber) состоит из тонких (5-60 микрон) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля - он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала (КВ, СВ и ДВ, УКВ, СВЧ или microwaves).

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические. Популярной средой является также витая пара. С помощью витой пары обычно подключают конечных абонентов сетей на расстояниях до 100 метров от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя - например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети. В таблице 1 приведены основные отличия разных типов кабелей.

Таблица 1 - Сетевые кабели

Характеристика	Тонкий коак-сиальный кабель	Толстый коаксиальный кабель	Витая пара	Оптоволоконный кабель
Эффективная длина кабеля	185 м	500м	100м	2км
Скорость передачи	10 Мбит/с	10 Мбит/с	$\geq$ 10 Мбит/с	$\geq$ 10 Мбит/с
Гибкость	Довольно гибкий	Менее гибкий	Самый гибкий	Не гибкий
Подверженность помехам	Хорошо защищен	Хорошо Защищен	Подвержен помехам	Не подвержен помехам

Варианты заданий на лабораторную работу

Проектируемая локальная вычислительная сеть должна быть для организации, располагающейся в нескольких зданиях (варианты представлены в таблице А.1).

Таблица А.1

Вариант	Количество зданий	Расстояние между зданиями, м	Количество этажей в зданиях	Число комнат на каждом этаже	Общее число компьютеров	Число используемых концентраторов
1	2	200	2	6	60	6
2	3	340	5	3	60	7
3	2	820	3	5	60	7
4	2	250	4	6	72	8
5	3	1420	2	5	50	5
6	1	230	5	2	50	5
7	2	200	4	2	40	4
8	2	720	4	3	60	8
9	3	250	3	6	54	5
10	4	1320	2	7	70	7
11	2	450	6	4	72	6
12	1	250	5	4	60	6
13	2	500	4	4	64	7
14	3	650	3	4	60	8
15	4	1250	2	4	40	4
16	3	400	6	3	54	5
17	2	200	7	2	70	7
18	1	500	1	3	45	4
19	2	120	7	3	63	7
20	3	430	6	2	60	6

Необходимо добиться максимальной эффективности использования сети по критерию цена-качество-скорость.

Составить схему ЛВС.

Подготовить отчет.

2.2 Лабораторная работа № 2 (2 часа)

Тема: «Способы коммутации»

2.2.1 Цель работы: изучить таблицу коммутации и Web-интерфейс коммутатора D-Link.

2.2.2 Задачи работы:

1. Изучить таблицу коммутации;

2. Изучить Web-интерфейс коммутатора D-Link.

2.2.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Рабочая станция;

2. Коммутатор DES-3200-10;

3. Кабель Ethernet;

4. Консольный кабель.

2.2.4 Описание (ход) работы:

Коммутатор (switch) — основное активное сетевое оборудование современныхлокальных сетей. В отличие от концентратора, коммутатор работает на канальном уровне модели OSI и передает кадры не на все порты, а непосредственно получателю, анализируя MAC-адрес источника/назначения.

Передача кадров коммутатором осуществляется на основе *таблицы коммутации*. Каждая запись в таблице коммутации состоит из номера порта и MAC-адреса. Как создаются записи в таблице коммутации? Например, если на порт 1 коммутатора поступает кадр от рабочей станции ПК1, то в таблице создается запись, ассоциирующая MAC-адрес рабочей станции ПК1 с номером входного порта. Таблица коммутации может строиться коммутатором автоматически, на основе динамического изучения MAC-адресов источников поступающих на порты кадров, или создаваться вручную администратором сети.

Коммутируемые сети имеют ряд особенностей и ограничений. Одной из главных проблем таких сетей, является увеличение широковещательных доменов. *Широковещательный домен* – это область распространения широковещательного трафика.Широковещательные кадры передаются на все узлы сети и могут привести к нерациональному использованию полосы пропускания. Для того, чтобы этого не происходило, нужно организовать небольшие широковещательные домены или *виртуальныелокальные сети (VLAN)*.

Виртуальной локальной сетью называется логическая группа узлов сети, трафиккоторой, в том числе и широковещательный, на канальном уровне полностью

изолирован от других узлов сети. Это значит, что передача кадров между разными виртуальными локальными сетями на основе MAC-адреса невозможна независимо от типа адреса — уникального, группового или широковещательного. В то же время, внутри виртуальной локальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с MAC-адресом назначения кадра.

Управление коммутатором через Web-интерфейс и изучение таблицы коммутации

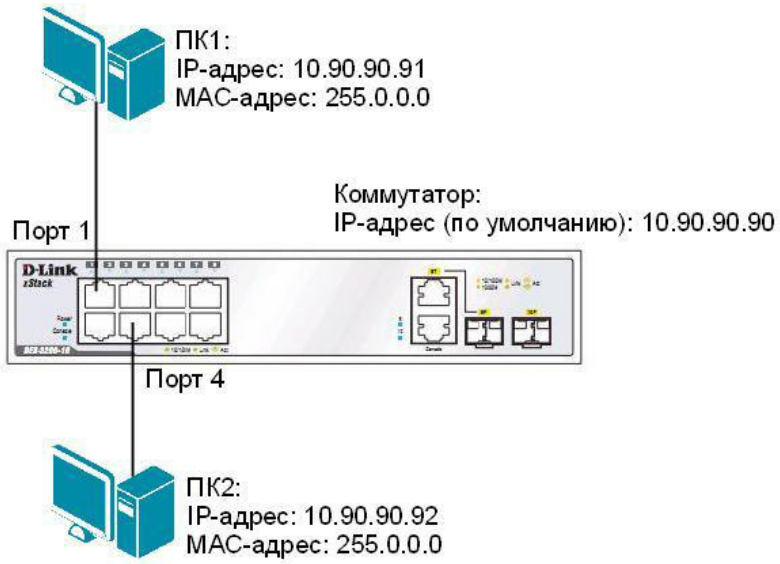


Рисунок 1.1 Схема сети

Шаг 1. Подключите ПК1 и ПК2 к коммутатору как показано на рис. 1.1.

Шаг 2. Настройте на рабочей станции ПК1 и ПК2 статический IP-адрес.

Шаг 3. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: ping 10.90.90.92

В командной строке ПК2 введите: ping 10.90.90.91

Шаг 4. Зайдите на Web-интерфейс коммутатора.

Чтобы зайти на Web -интерфейс коммутатора, выполните следующие действия:

1. На рабочей станции ПК1 запустите Web-браузер (Internet Explorer, Mozilla Firefox), в адресной строке которого укажите IP-адрес интерфейса управления коммутатора по умолчанию:

http://10.90.90.90

Внимание: IP-адрес управления коммутатора по умолчанию обычно указывается в руководствепользователя. Для коммутатора D-Link DES-3200-10 IP-адрес управления по умолчанию — 10.90.90.90

2. В появившемся окне аутентификации, поля *User name* и *Password* оставьте пустыми и нажмите *Ок*. После этого появится окно Web-интерфейса управления коммутатора (рис.

1.2).

Если на рабочей станции произведены настройки прокси-сервера, то их нужно отключить.

Для Mozilla Firefox: меню *Инструменты → Настройки → Дополнительные*. Далее вкладка *Сеть →Настройка параметров соединения Firefox с Интернетом → Настроить → Без прокси*.

Для Internet Explorer: меню *Сервис → Свойство обозревателя*. Далее вкладка *Подключения →Настройка сети → Автоматическое определение параметров*.

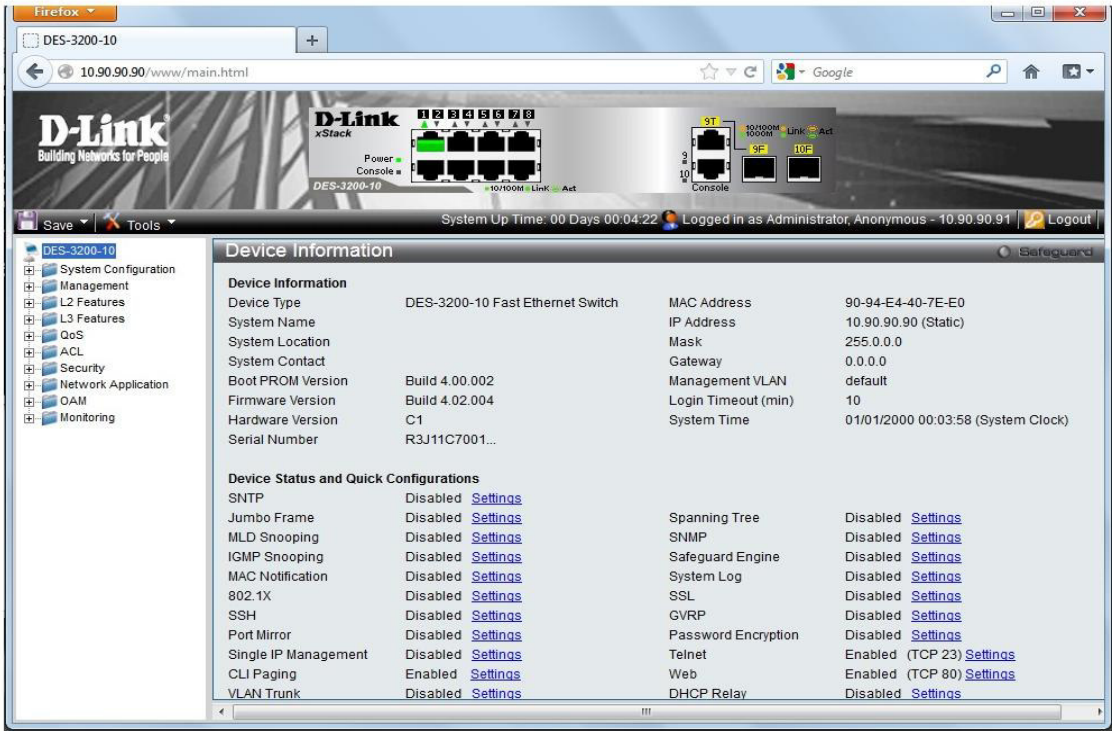


Рисунок 1.2 Web-интерфейс управления коммутатора DES-3200-10

Шаг 5. Посмотрите содержимое таблицы коммутации. В левой части окна выберите*L2Features → FDB → MAC Address Table* (рис. 1.3).

Сколько записей наблюдаете? _____

Какой тип (type) у каждой записи в таблице коммутации? _____

Шаг 6. Отключите рабочую станцию ПК2 от 4 порта и подключите к 5 порту.

Шаг 7. Посмотрите содержимое таблицы коммутации. Что изменилось? _____

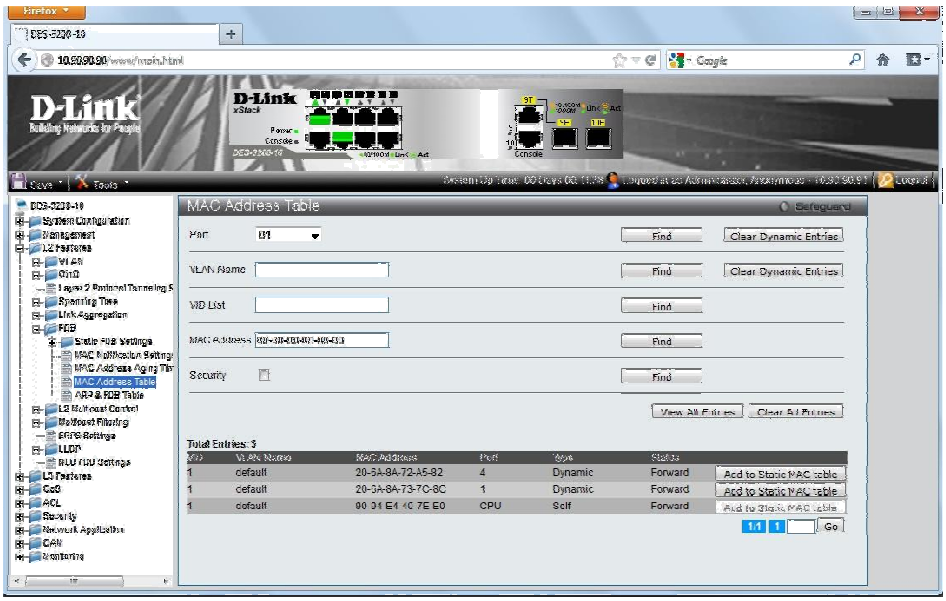


Рисунок 1.3 Таблица коммутации

Шаг 8. Создайте статическую запись в таблице коммутации для ПК2 на порте 5. Для этогонажмите на кнопку *Add to Static MAC table* (рис. 1.4).

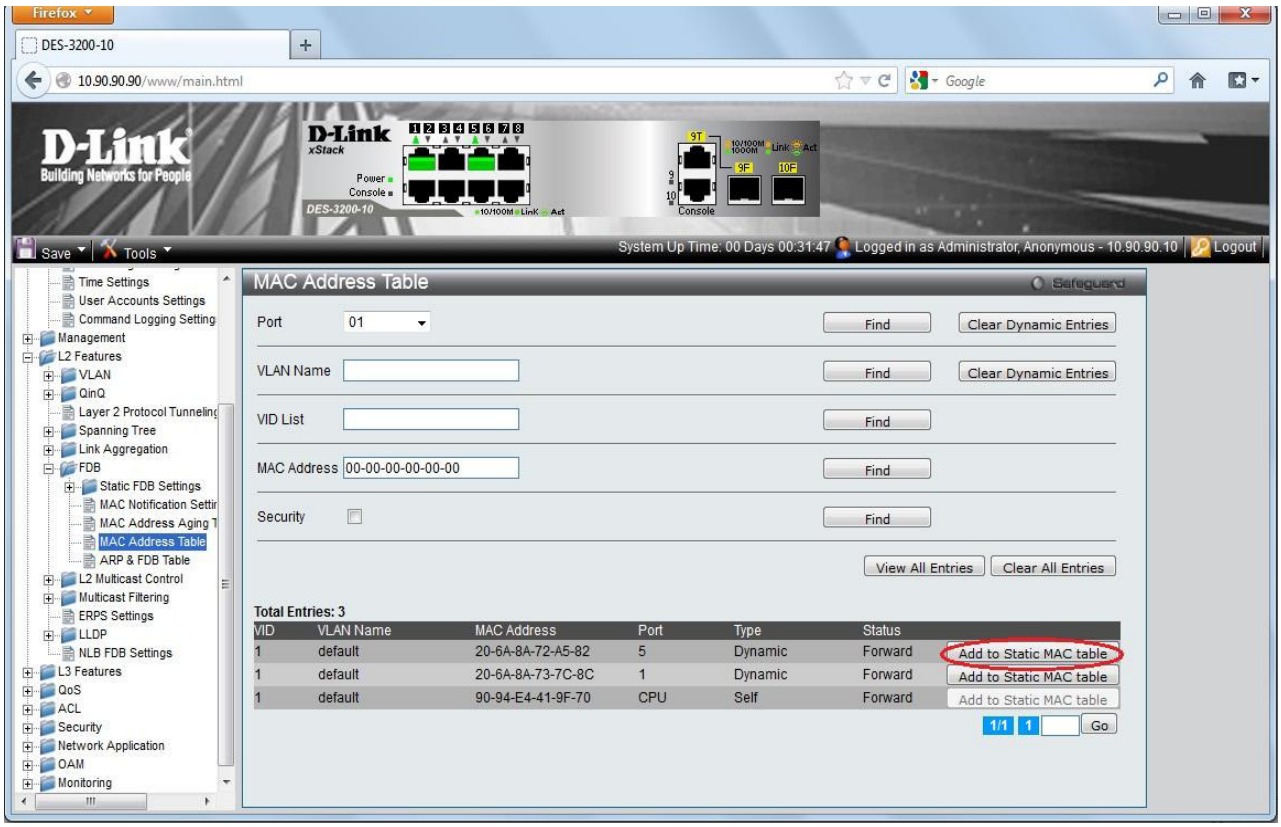


Рисунок 1.4 Создание статической записи

Шаг 9. Отключите рабочую станцию ПК2 от 5 порта и подключите к 4 порту.

Шаг 10. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1введите: ping 10.90.90.92

В командной строке ПК2 введите: ping 10.90.90.91

Объясните, почему нет связи между ПК1 и ПК2 _____

Шаг 11. Удалите статическую запись из таблицы коммутации. Влевойчастиокнавыберите *FDB → Static FDB Settings → Unicast Static FDB Settings*.В правой части окна нажмите *Delete* напротив записи для ПК2 (рис. 1.5).

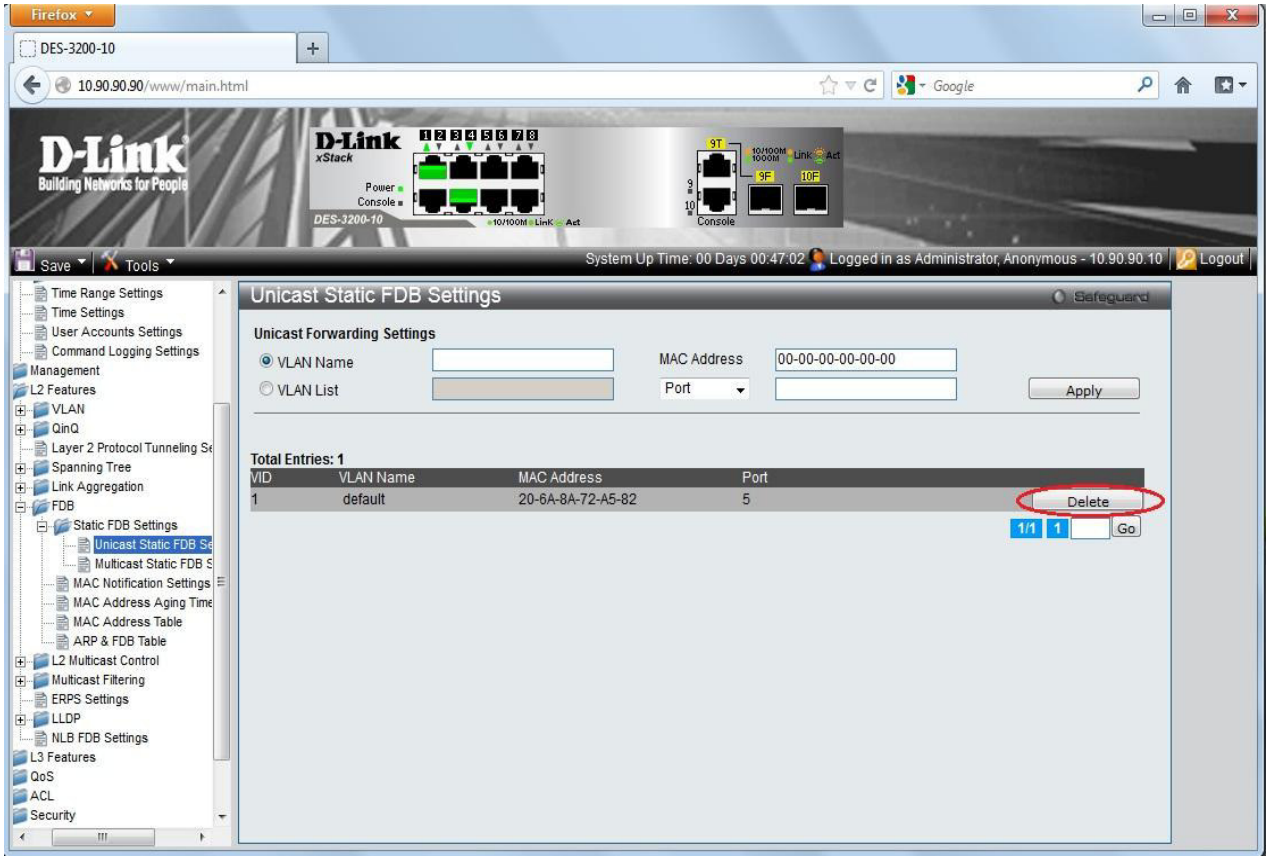


Рисунок 1.5 Удаление статической записи

Шаг 12. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1введите: ping 10.90.90.92

В командной строке ПК2 введите: ping 10.90.90.91

Шаг 13. Сбросьте настройки коммутатора к заводским настройкам по умолчанию. Выберите

*Tools → Reset → ResetConfig*инажмите*Apply*.

Диагностика сети во время широковещательного шторма

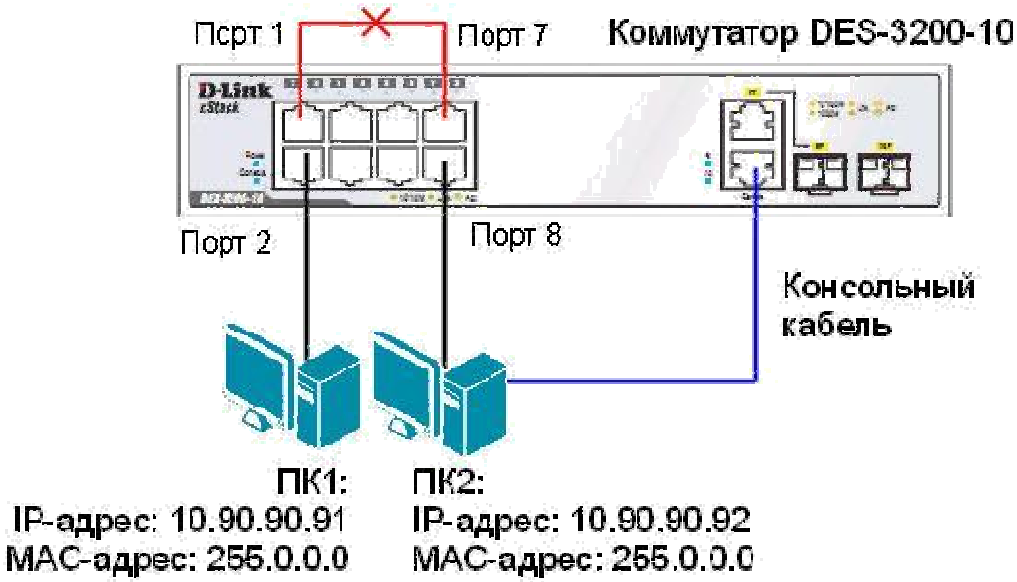


Рисунок 1.6 Схема сети

Управление коммутатором осуществляется не только через Web-интерфейс. Для более тонкой настройки устройства используется управление через интерфейс командной строки (Command Line Interface, CLI). Доступ к интерфейсу командной строки коммутатора осуществляется путем подключения к его консольному порту персонального компьютера с установленной программой эмуляции терминала.

Шаг 1. Подключите ПК2 к консольному порту коммутатора с помощью кабеля RS-232.После подключения к консольному порту коммутатора, на персональном компьютере запустите программу эмуляции терминала VT100 (например, *putty.exe* или программу *HyperTerminal* в Windows XP).

В программе HyperTerminal установите следующие параметры подключения:

Скорость (бит/с):	115200
Биты данных:	8
Чётность:	нет
Стоповые биты:	1
Управление потоком:	нет

В программе *Putty* установите следующие параметры подключения:

1. В категории *Session* выберите *Serial* и установите скорость 115200 (рис. 1.7);

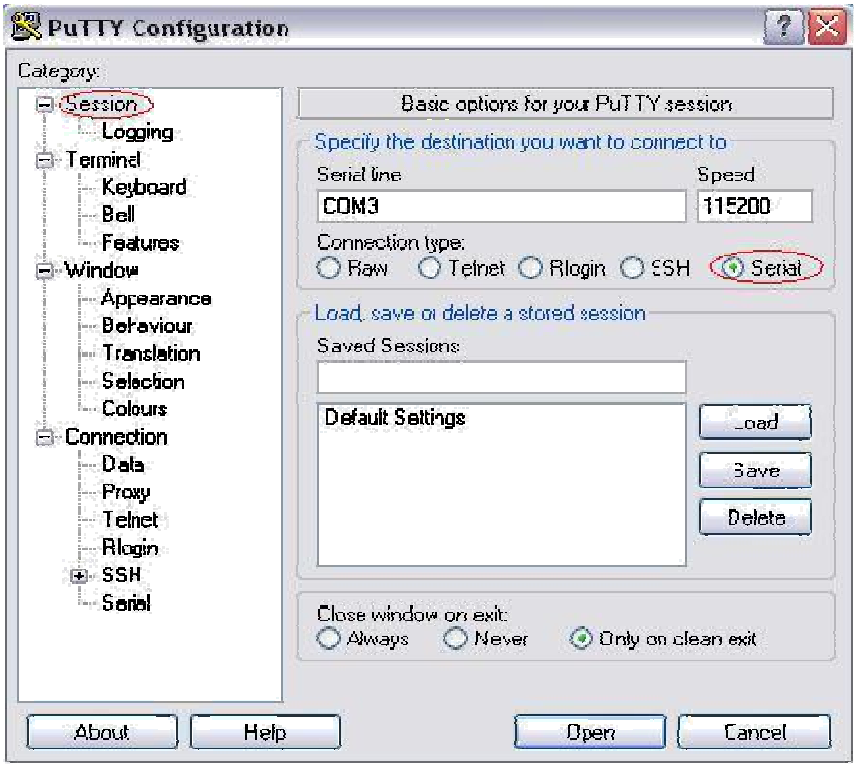


Рисунок 1.7 Интерфейс программы putty.exe

2. В категории *Translation* установите *UTF-8* и нажмите *Open* (рис. 1.8);

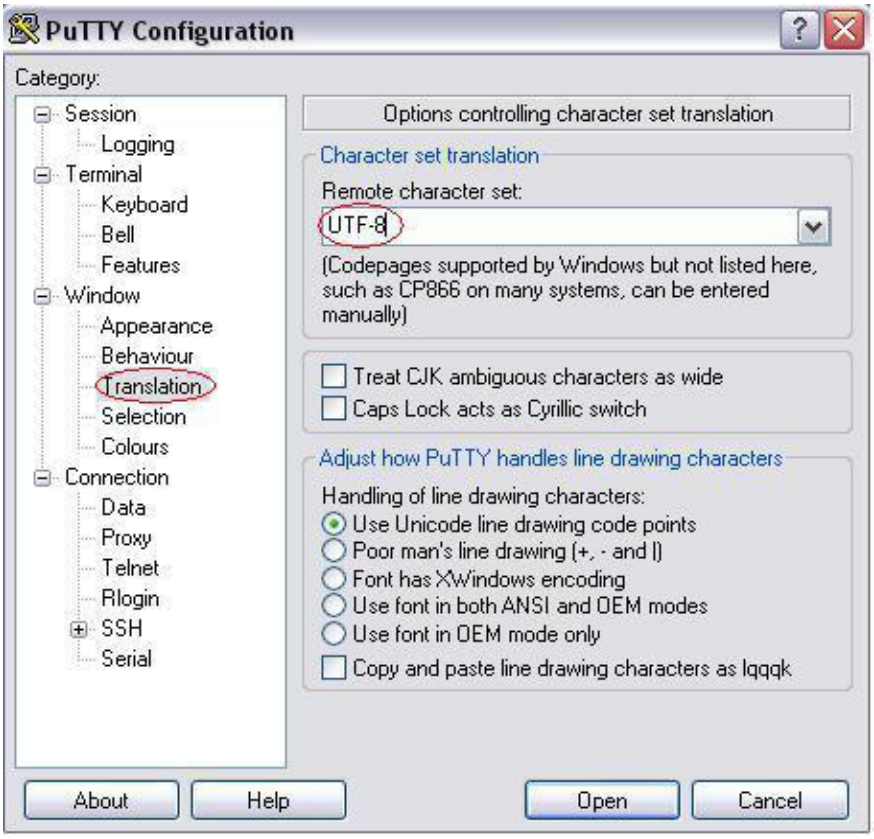


Рисунок 1.8 Интерфейс программы putty.exe

3. Нажмите кнопку *Open*. В открывшемся окне нажмите клавишу *Enter* (рис. 1.9).

Примечание: По умолчанию на коммутаторе UserName и PassWord не определены, поэтому два раза нажмите клавишу Enter.

После этого появится приглашение для ввода команд: DES-3200-10:admin#

Рисунок 1.9 Окно эмуляции терминала VT100

Внимание: при написании команд в CLI важно учитывать регистр. Для того чтобыознакомиться с правильностью написания команд, последовательностью выполнения операций можно обращаться к встроенной помощи по командам!

Примечание: не соединяйте порты коммутатора одним кабелем до особого указания.

Шаг 2. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1введите: ping 10.90.90.92

В командной строке ПК2 введите: ping 10.90.90.91

Шаг 3. Посмотрите загрузку портов

коммутатора:show utilization ports

Какая загрузка портов, используемых в схеме?

Порт 1% _____

Порт 2% _____

Порт 7% _____

Порт 8% _____

Шаг 4. Соберите схему и соедините кабелем Ethernet порты 1 и 7 коммутатора.

Шаг 5. Посмотрите загрузку портов

коммутатора:show utilization ports

Что вы наблюдаете? Возник широковещательный шторм? Почему?

_____

Какая теперь загрузка портов, используемых в схеме?

Порт 1% _____

Порт 2% _____

Порт 7% _____

Порт 8%_____

Шаг 6. Выполните на рабочей станции ПК1

команду:ping 10.90.90.92

Что вы наблюдаете? Объясните почему нет связи между рабочими станциями?

_____

Шаг 7. Удалите коммутационную петлю, отключив кабель от портов 1 и 7.

Шаг 8. Добавьте порты 2 и 8 в

новуюVLAN:config vlan default delete 2, 8

create vlan v2 tag 2

config vlan v2 add untagged 2,8

Шаг 9. Посмотрите загрузку портов

коммутатора:show utilization ports

Какая загрузка портов, используемых в схеме?

Порт 1% _____

Порт 2% _____

Порт 7% _____

Порт 8% _____

Шаг 10. Соедините кабелем Ethernet порты 1 и 7 коммутатора.

Шаг 11. Посмотрите загрузку портов

коммутатора:show utilization ports

Что вы наблюдаете? Почему нет широковещательного шторма на портах 2 и 6?

Шаг 12. Выполните на рабочей станции ПК1 команду:ping 10.90.90.92

Что вы наблюдаете? Объясните почему? _____

2.3 Лабораторная работа № 3 (2 часа)

Тема: «Характеристики линии связи»

2.3.1 Цель работы: изучить основные характеристики линий связи.

2.3.2 Задачи работы:

1. ознакомиться с основными характеристиками каналов связи.

2.3.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер, включенный в сеть IP, Microsoft Windows.

2.3.4 Описание (ход) работы:

К основным характеристикам канала (линии) связи существенно влияющим на качество передачи сигнала можно отнести:

- полосу пропускания;
- затухание;

- помехоустойчивость;
- пропускную способность;
- достоверность передачи данных.

Полоса пропускания

Полоса пропускания (*bandwidth*) – диапазон частот, в пределах которого амплитудно-частотная характеристика (АЧХ) канала (линии) связи достаточно равномерна для того, чтобы обеспечить передачу сигнала без существенного искажения его формы.

Ширина полосы пропускания F определяется как разность верхней $f_в$ и нижней $f_н$ граничных частот участка АЧХ, на котором мощность сигнала уменьшается не более чем в 2 раза по сравнению с максимальным значением: $F=f_в - f_н$ (что приблизительно соответствует −3 дБ).

Измеряется полоса пропускания в герцах (Гц).

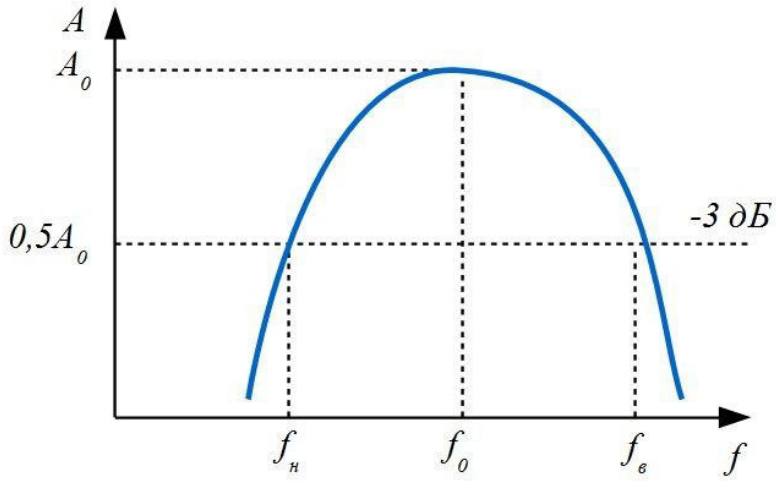


Рис. 1. Полоса пропускания канала связи

Ширина полосы пропускания существенным образом влияет на максимально возможную скорость передачи информации по каналу связи и зависит от типа среды передачи, наличия в каналах частотных фильтров.

Сигналы составлены из большого набора гармоник, однако приемник может получить лишь те гармоники, частоты которых находятся внутри полосы пропускания канала. Чем шире полоса пропускания канала, тем выше может быть скорость передачи данных и тем более высокочастотные гармоники сигнала могут передаваться. Если в полосу пропускания канала попадают гармоники, амплитуды которых вносят основной вклад в результирующий сигнал, форма сигнала претерпит незначительные изменения, и сигнал будет правильно распознан приемником.

В противном случае форма сигнала будет значительно искажаться, что приведет к снижению скорости передачи информации по каналу вследствие проблем с его распознаванием, которые вызовут ошибки связи и повторные передачи.

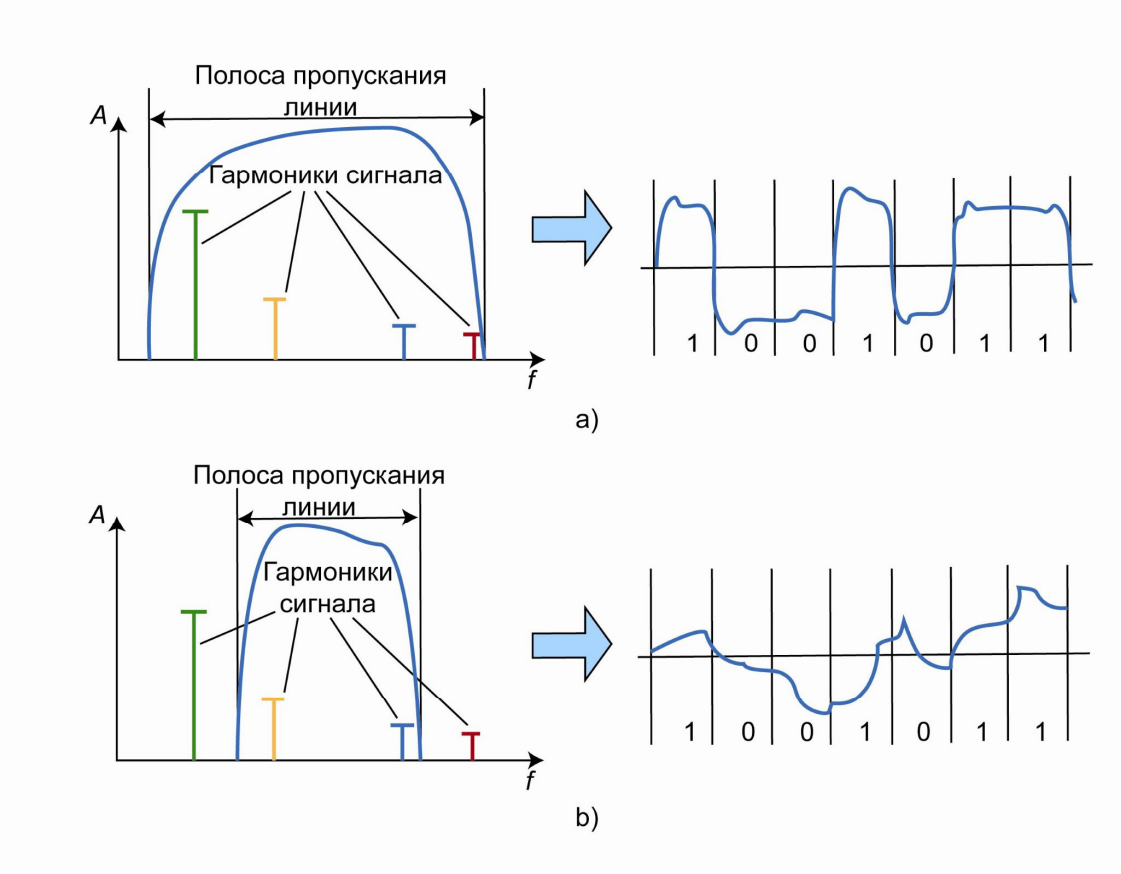


Рис. 2. Влияние полосы пропускания на сигнал

Затухание

При передаче сигнала по каналу связи, происходит его постепенное ослабление (*затухание*), что обусловлено физическими и техническими свойствами среды передачи и используемых сетевых устройств. Для корректного распознавания сигнала в точке приема это ослабление не должно превышать некоторой пороговой величины.

Затухание (*attenuation*) — это величина, показывающая, насколько уменьшается мощность (амплитуда) сигнала на выходе канала связи по отношению к мощности (амплитуде) сигнала на входе. Коэффициент затухания *d* измеряется в децибелах (дБ, dB) на единицу длины и вычисляется по следующей формуле:

$$d[\text{дБ}] = 10 \lg \frac{P_{вых}}{P_{вх}},$$

где $P_{вых}$ – мощность выходного сигнала; $P_{вх}$ – мощность входного сигнала.

Затухание характерно как для аналоговых, так и для цифровых сигналов. Оно увеличивается с ростом частоты сигнала: чем выше частота, тем сильнее сигнал подвержен затуханию. По этой причине приемникам высокоскоростного оборудования значительно сложнее распознать исходный сигнал.

Затухание сигнала влияет на расстояние, которое он может пройти между двумя точками без усиления или восстановления. Затухание является одним из важных параметров определенных для кабелей (витой пары, волоконно-оптического, коаксиального). Чем меньше затухание, тем более качественным является кабель. Поэтому при проектировании проводных каналов связи надо учитывать характеристики кабелей и использовать кабели с наименьшим значением затухания для достижения максимальной длины канала.

Помехоустойчивость

В реальном канале связи существуют помехи, обусловленные характеристиками среды передачи, каналообразующей аппаратуры, влиянием электромагнитных полей различных электронных устройств. В результате действия различных помех в канале связи появляются ошибки.

Одним из важнейших показателей канала связи является его **помехоустойчивость**, под которой понимают способность канала противостоять воздействию помех. Помехоустойчивость основывается на возможности отличить сигнал от помехи с заданной достоверностью, поэтому при построении канала связи нужно учитывать возможные помехи и предельно использовать различие между ними и сигналом.

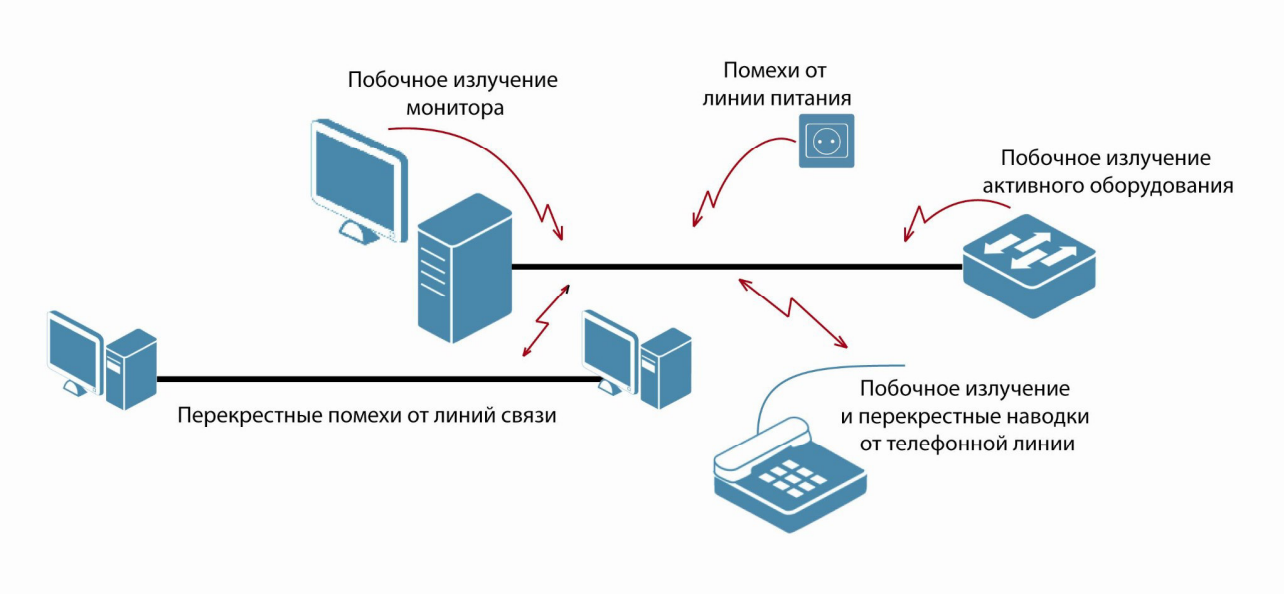


Рис. 4. Влияние помех на канал связи

В зависимости от источника возникновения и от характера их воздействия помехи делятся на внутренние, внешние и взаимные. *Внутренние помехи* или шумы возникают от источников находящихся в данном канале связи и появляются сразу же после включения оборудования связи. Они в основном определяются тепловыми, дробовыми, контактными и импульсными шумами и практически неустранимы.

Внешние помехи делятся на промышленные, радиопомехи, атмосферные и космические. Промышленные помехи (*электромагнитная интерференция*, Electro Magnetic Interference (EMI)) создаются в результате влияния на канал связи электромагнитных полей различных электрических устройств: ламп дневного света, бытовых приборов, компьютеров, радиосистем, линий электропередач, электрооборудования промышленных предприятий, медицинских установок, контактных сетей электрифицированного транспорта (трамвая, троллейбуса и т.п.), световой рекламы на газоразрядных лампах и т.п.

Радиопомехи (*радиочастотная интерференция*, Radio Frequency Interference (RFI)) возникают от излучения радиостанций различного назначения, спектр которых по какимлибо причинам накладывается на спектр полезных сигналов канала связи.

К атмосферным помехам относятся помехи, вызванные различными атмосферными явлениями: магнитными бурями, северными сияниями, грозовыми разрядами и т.д. К космическим помехам относятся электромагнитные помехи, создаваемые излучениями Солнца, видимых и невидимых звезд, туманностей в соответствующих диапазонах частот.

Взаимные (перекрестные, cross talk*)помехи* или наводки возникают при передаче информации по смежным каналам сигнал, переданный по одному каналу связи, создает нежелательный эффект в другом (возникает интерференция сигналов).

Наименее защищенными от влияния помех являются беспроводные каналы связи. На них действуют как внешние, так и перекрестные помехи. В беспроводных домашних сетях внешние помехи возникают от работающих микроволновых печей, компьютеров, сотовых телефонов и т.д. А перекрестные наводки связанны с помехами от другого беспроводного оборудования, работающего на той же частоте. Это особенно актуально в многоквартирных домах, где домашние сети в основном построены с использованием беспроводных технологий.

Среди кабельных каналов наиболее подвержены влиянию помех каналы на основе электрических кабелей. Для борьбы с помехами разработчики электрических кабелей используют: э*кранирование* (shielding) и *скручивание проводников*. Экранирование используется для защиты от электромагнитных и радиопомех. Экран представляет собой металлическую оплетку или фольгу, которая окружает каждый провод или группу проводов в кабеле. Он действует как барьер для взаимодействующих сигналов.

Электрические кабели сами являются источником электромагнитного излучения, которое может вызывать перекрестные помехи. В кабелях на основе витой пары эти помехи известны как *перекрестные наводки на ближнем конце* (Near End Cross Talk, NEXT) и *перекрестные наводки на дальнем конце* (Far End Cross Talk, FEXT) и связаны с взаимным влиянием электромагнитных полей сигналов, передаваемых по разным парам проводников. Для подавления этих электромагнитных полей используется скручивание проводников витой пары.

Наиболее защищенными от помех являются оптические каналы. На волоконнооптические кабели не воздействуют электромагнитные помехи (EMI), радиочастотные помехи (RFI), молнии и скачки высокого напряжения. Также волоконно-оптические кабели не создают никаких электромагнитных или радиочастотных помех.

Чтобы шумы заметно не снижали качества передачи их влияние необходимо ограничивать. Методы борьбы с шумами заключаются в обеспечении такого уровня сигнала в месте приема, который бы обеспечил требуемое качество принимаемого сигнала.

Одним из важных параметров канала связи, позволяющим оценить мешающее воздействие помех на сигнал является **отношение сигнал/шум** (*SNR, Signal-to-Noise Ratio*). Оно определяется как отношение мощности сигнала P_c к мощности шума (помех) $P_ш$ и выражается в децибелах (дБ):

$$SRN\ [\text{дБ}] = 10 \lg\left(\frac{P_c}{P_ш}\right),$$

где P_c – мощность сигнала; $P_ш$ - мощность шума (помех).

При этом чем больше отношение сигнал/шум, тем меньше шум влияет на полезный сигнал при его передаче по каналу связи и ведет к хорошему распознаванию сигнала приемником.

Для повышения помехоустойчивости канала связи применяются следующие методы:

- увеличение отношения сигнал/шум;
- расширение спектра сигнала;
- увеличение избыточности информации; применение помехоустойчивых кодов; фильтрация полезного сигнала.

Пропускная способность

Пропускная способность (*throughput*) канала связи максимально возможная *информационная* скорость передачи данных количество данных, которое может быть передано по каналу связи за единицу времени. Измеряется пропускная способность в битах в секунду (бит/с или bps bits per second).

Максимальная пропускная способность зависит от полосы пропускания канала связи и отношения сигнал/шум и может быть рассчитана по формуле Клода Шеннона:

$$C = F \log_2\left(1 + \frac{P_c}{P_ш}\right),$$

где C – максимальная пропускная способность канала (бит/с); F – ширина полосы пропускания канала (Гц); P_c – мощность сигнала; $P_ш$ – мощность шума (помехи).

Как видно из формулы, пропускная способность канала может быть повышена за счет увеличения полосы пропускания F или увеличение отношения сигнал/шум. При этом первый способ более эффективен и менее трудоемок по сравнению со вторым, в связи с логарифмической зависимостьюC от $P_c/ P_ш$.

Реальная скорость передачиданных по каналу связи обычно *меньше* его *пропускной способности* и зависит от параметров каналообразующей аппаратуры, способов организации передачи данных, количества узлов, подключенных к каналу связи. Также на снижение скорости влияют накладные расходы, связанные с передачей по сети служебных сообщений, которые требуется для работы сетевых протоколов.

Следует понимать различие между информационной скоростью и символьной скоростью. *Информационная скорость* (information rate, bitrate) – это скорость передачи битов, измеряемая в бит/с и производных единицах. *Символьная скорость* (symbol rate) или *скорость модуляции* – это скорость изменения символов, измеряемая в бодах или символах в секунду. Каждый символ представляет один или несколько битов информации в зависимости от выбранного способа их кодирования.

2.4 Лабораторная работа №4 (2 часа).

Тема: «Сетевая модель OSI»

2.4.1 Цель работы: изучить правила адресации сетевого уровня, научиться распределять адресамежду участниками сети передачи данных и организовывать маршрутизацию между сегментами сети. Изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети.

2.4.2 Задачи работы:

1. изучить сетевую модель OSI;
2. изучить правила адресации сетевого уровня на примере протокола IP;
3. изучить маршрутизацию IP.

2.4.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. персональный компьютер, включенный в сеть IP, Microsoft Windows.

2.4.4 Описание (ход) работы:

Модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами. Модель не включает средства взаимодействия приложений конечных пользователей.

Эта модель описывает функции семи иерархических уровней и интерфейсы взаимодействия между уровнями. Каждый уровень определяется сервисом, который он предоставляет вышестоящему уровню, и протоколом - набором правил и форматов данных для взаимодействия между собой объектов одного уровня, работающих на разных компьютерах.

Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями. Ниже перечислены (в направлении сверху вниз) уровни модели OSI и указаны их общие функции.

Уровень приложения (Application) - интерфейс с прикладными процессами.

Уровень представления (Presentation) - согласование представления (форматов, кодировок) данных прикладных процессов.

Сеансовый уровень (Session) - установление, поддержка и закрытие логического сеанса связи между удаленными процессами.

Транспортный уровень (Transport) - обеспечение безошибочного сквозного обмена потоками данных между процессами во время сеанса.

Сетевой уровень (Network) - фрагментация и сборка передаваемых транспортным уровнем данных, маршрутизация и продвижение их по сети от компьютера-отправителя к компьютеру-получателю.

Канальный уровень (Data Link) - управление каналом передачи данных, управление доступом к среде передачи, передача данных по каналу, обнаружение ошибок в канале и их коррекция.

Физический уровень (Physical) - физический интерфейс с каналом передачи данных, представление данных в виде физических сигналов и их кодирование.

Принципы выделения этих уровней таковы: каждый уровень отражает надлежащий уровень абстракции и имеет строго определенную функцию. Эта функция выбиралась, прежде всего, так, чтобы можно было определить международный стандарт. Границы уровней выбирались так, чтобы минимизировать поток информации через интерфейсы.

Два самых низших уровня - физический и канальный - реализуются аппаратными и программными средствами, остальные пять более высоких уровней реализуются, как правило, программными средствами (рисунок 1).

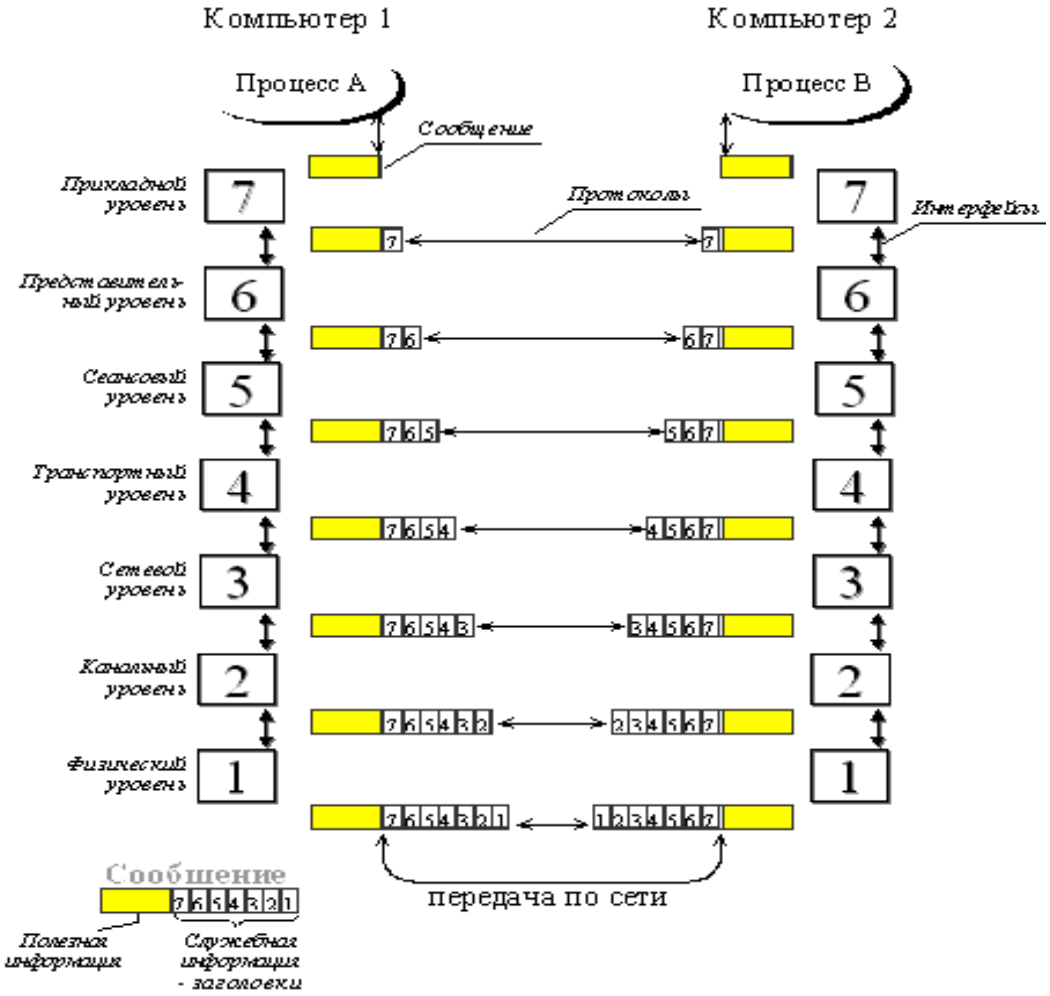


Рисунок 1 - Модель взаимодействия открытых систем ISO/OSI

При продвижении пакета данных по уровням сверху вниз каждый новый уровень добавляет к пакету свою служебную информацию в виде заголовка и, возможно, трейлера (информации, помещаемой в конец сообщения). Эта операция называется инкапсуляцией данных верхнего уровня в пакете нижнего уровня. Служебная информация предназначается для объекта того же уровня на удаленном компьютере, ее формат и интерпретация определяются протоколом данного уровня. Наконец, сообщение достигает нижнего, физического уровня, который, собственно, и передает его по линиям связи машине-адресату. К этому моменту сообщение "обрастает" заголовками всех уровней.

Когда сообщение по сети поступает на другую машину, оно последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует, обрабатывает и удаляет заголовок своего уровня, выполняет соответствующие данному уровню функции и передает сообщение вышележащему уровню. Тот в свою очередь рассматривает эти данные как пакет со своей служебной информацией и данными для верхнего уровня, и процедура повторяется, пока пользовательские данные, очищенные от всей служебной информации, не достигнут прикладного процесса.

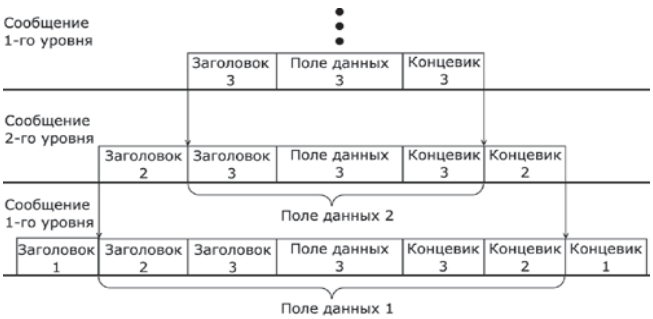


Рисунок 2 – Вложенность сообщений различных уровней

Кроме термина "сообщение" (message) существуют и другие названия, используемые сетевыми специалистами для обозначения единицы обмена данными. В стандартах ISO для протоколов любого уровня используется такой термин как "протокольный блок данных" - Protocol Data Unit (PDU). Кроме этого, часто используются названия кадр (frame), пакет (packet), дейтаграмма (datagram).

Теперь рассмотрим каждый уровень этой модели. Отметим что это модель, а не архитектура сети. Она не определяет протоколов и сервис каждого уровня. Она лишь говорит, что он должен делать.

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

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

В обобщенном виде функции физического уровня заключаются в следующем:

- передача битов по физическим каналам;
- формирование электрических сигналов;
- кодирование информации;
- синхронизация;
- модуляция.

Этот уровень реализуется аппаратно. Примером протокола физического уровня может служить спецификация 10Base-T технологии Ethernet.

Канальный уровень. На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются (разделяются) попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит в начало и конец каждого кадра, чтобы отметить его, а также вычисляет контрольную сумму, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Необходимо отметить, что функция исправления ошибок для канального уровня не является обязательной, поэтому в некоторых протоколах этого уровня она отсутствует, например в Ethernet и Frame relay.

Функции канального уровня заключаются в следующем:

- надежная доставка пакета между двумя соседними станциями в сети с произвольной топологией, а также между любыми станциями в сети с типовой топологией;
- проверка доступности разделяемой среды;
- выделение кадров из потока данных, поступающих по сети;
- формирование кадров при отправке данных;
- подсчет и проверка контрольной суммы.

Этот уровень реализуются программно-аппаратно. В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда. Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

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

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень обеспечивает обмен сообщениями между двумя соседними компьютерами, соединенными индивидуальной линией связи. Примерами протоколов "точка - точка" могут служить широко распространенные протоколы PPP и LAP-B.

Именно так организованы сети X.25. Иногда в глобальных сетях функции канального уровня в чистом виде выделить трудно, так как в одном и том же протоколе они объединяются с функциями сетевого уровня. Примерами такого подхода могут служить протоколы технологий ATM и Frame relay.

В целом канальный уровень представляет собой весьма мощный набор функций по пересылке сообщений между узлами сети.

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Функции сетевого уровня достаточно разнообразны. Рассмотрим их на примере объединения локальных сетей.

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

На сетевом уровне сам термин "сеть" наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Маршрутизатор — это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или хопов (от слова hop — прыжок), каждый раз выбирая подходящий

маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Свойства сетевого уровня — доставка пакета:

- между любыми двумя узлами сети с произвольной топологией;
- между любыми двумя сетями в составной сети.

При этом, сеть — это совокупность компьютеров, использующих для обмена данными единую сетевую технологию; а маршрут — последовательность прохождения пакетом маршрутизаторов в составной сети.

На рисунке 3 показаны четыре сети, связанные тремя маршрутизаторами. Между узлами A и B данной сети пролегает два маршрута: первый — через маршрутизаторы 1 и 3, а второй — через маршрутизаторы 1, 2 и 3.

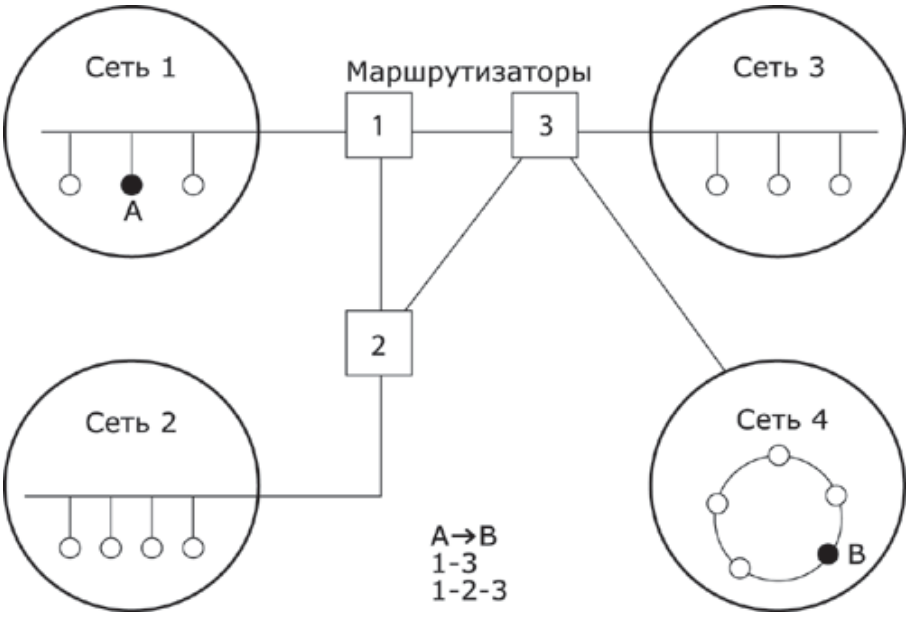


Рисунок 3 - Пример составной сети

В общем случае функции сетевого уровня шире, чем функции передачи сообщений по связям с нестандартной структурой, которые мы рассмотрели на примере объединения нескольких локальных сетей. Сетевой уровень также решает задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Сообщения сетевого уровня принято называть пакетами (packet). При организации доставки пакетов на сетевом уровне используется понятие "номер сети". В этом случае адрес получателя состоит из старшей части — номера сети и младшей — номера узла в этой сети. Все узлы одной сети должны иметь одну и ту же старшую часть адреса, поэтому термину

"сеть" на сетевом уровне можно дать и другое, более формальное, определение: сеть — это совокупность узлов, сетевой адрес которых содержит один и тот же номер сети.

На сетевом уровне определяется два вида протоколов. Первый вид — сетевые протоколы (routed protocols) — реализуют продвижение пакетов через сеть. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто протоколами маршрутизации (routing protocols). С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют протоколами разрешения адресов — Address Resolution Protocol, ARP. Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют сути.

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

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

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней, а с другой стороны, этот выбор зависит от того, насколько надежной является вся система транспортировки данных в сети. Так, например, если качество каналов передачи связи очень высокое, и вероятность возникновения ошибок, не обнаруженных протоколами более низких уровней, невелика, то

разумно воспользоваться одним из облегченных сервисов транспортного уровня. Если же транспортные средства изначально очень ненадежны, то целесообразно обратиться к наиболее развитому сервису транспортного уровня, который работает, используя максимум средств для обнаружения и устранения ошибок - с помощью предварительного установления логического соединения, контроля доставки сообщений с помощью контрольных сумм и циклической нумерации пакетов, установления тайм-аутов доставки и т.п.

Т.о. функции транспортного уровня - это обеспечение доставки информации с требуемым качеством между любыми узлами сети:

- разбивка сообщения сеансового уровня на пакеты, их нумерация;
- буферизация принимаемых пакетов;
- упорядочивание прибывающих пакетов;
- адресация прикладных процессов;
- управление потоком.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети - компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell.

Протоколы четырех нижних уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Остальные три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Сеансовый уровень. Сеансовый уровень (Session layer) обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Функции сеансового уровня - это управление диалогом объектов прикладного уровня:

- установление способа обмена сообщениями (дуплексный или полудуплексный);
- синхронизация обмена сообщениями;
- организация "контрольных точек" диалога.

Уровень представления. Этот уровень обеспечивает гарантию того, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе.

При необходимости уровень представления выполняет преобразование форматов данных в некоторый общий формат представления, а на приеме, соответственно, выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером протокола, работающего на уровне представления, является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Уровень представления согласовывает представление (синтаксис) данных при взаимодействии двух прикладных процессов:

– преобразование данных из внешнего формата во внутренний;
– шифрование и расшифровка данных.

Прикладной уровень. Прикладной уровень - это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется *сообщением (message)*.

Существует очень большое разнообразие протоколов прикладного уровня. Среди них хотелось бы отметить такие как FTP, Telnet, HTTP.

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

Прикладной уровень - это набор всех сетевых сервисов, которые предоставляет система конечному пользователю:

- идентификация, проверка прав доступа;
- принт- и файл-сервис, почта, удаленный доступ.

Три нижних уровня - физический, канальный и сетевой - являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием.

Три верхних уровня - сеансовый, уровень представления и прикладной - ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних уровней. Это позволяет разрабатывать

приложения, независящие от технических средств, непосредственно занимающихся транспортировкой сообщений.

Рисунок 4 показывает уровни модели OSI, на которых работают различные элементы сети. Компьютер, с установленной на нем сетевой ОС, взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства. В зависимости от типа, коммуникационное устройство может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост и коммутатор), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор).

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, сервисами, предоставляемыми на верхних уровнях и прочими параметрами.

Поэтому модель OSI стоит рассматривать, в основном, как опорную базу для классификации и сопоставления протокольных стеков.

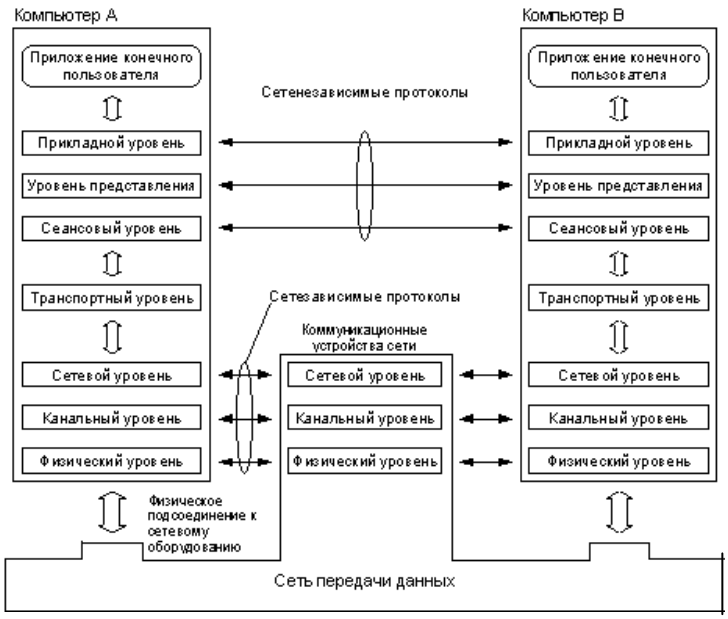


Рисунок 4 - Сетезависимые и сетенезависимые уровни модели OSI

Протокол IP

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP» означает «набор протоколов, связанных с IP и TCP(протоколом транспортного уровня)».

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из

соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети.

Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол.

Таким образом, две машины, подключенные *к одной подсети*, могут обмениваться пакетами.

Когда необходимо передать пакет между машинами, *подключенными к разнымподсетям*, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключенк подсети также как обычный узел). Оттуда пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель: там пакет направляется к получателю.

Таким образом, адрес получателя должен содержать в себе:

- номер (адрес) подсети;
- номер (адрес) участника (хоста) внутри подсети.

IP адреса представляют собой 32-х разрядные двоичные числа. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса (для удобства будем записывать точки и в двоичном изображении).

192.168.200.47 является десятичным эквивалентом двоичного Адреса

11000000.10101000.11001000.00101111

Иногда применяют десятичное значение IP-адреса. Его легко вычислить

Двоичное	Десятичное
10000000	**128**
11000000	**192**
11100000	**224**
11110000	**240**
11111000	**248**
11111100	**252**
11111110	**254**
11111111	**255**

$192*256^3+168*256^2+200*256+47=3232286767$

или с помощью метода Горнера :

(((192*256)+168)*256+200)*256+47=3232286767

Количество разрядов *адреса подсети* может быть различным и определяется *маской сети*.

Маска сети также является 32-х разрядным двоичным числом. Разряды маски имеютследующий смысл: если разряд маски равен 1, то соответствующий разряд адреса является разрядом адреса подсети, а если 0, то разрядом хоста внутри подсети. Все единичные разряды маски (если они есть) находятся в старшей (левой) части маски, а нулевые (если они есть) – в правой (младшей).

Исходя из вышесказанного, маску часто записывают в виде числа единиц в ней содержащихся.

255.255.248.0 (11111111.11111111.11111000.00000000) – являетсяправильноймаской подсети **(/21)**, а **255.255.250.0 (11111111.11111111.1111101<u>0</u>.00000000)** – являетсянеправильной,недопустимой.

Нетрудно увидеть, что *максимальный размер подсети* может быть только степенью двойки (двойку надо возвести в степень, равную количеству нулей в маске).

При передаче пакетов используются *правила маршрутизации*, главное из которых звучит так: «Пакеты участникам своей подсети доставляются напрямую, а остальным – по другим правилам маршрутизации».

Таким образом, требуется определить, является ли получатель членом нашей подсети или нет.

1. ***Определение диапазона адресов подсети.***

Определение диапазона адресов подсети можно произвести из определения понятия маски:

В те разряды, которые относятся к адресу подсети, у всех хостов подсети должны быть *одинаковы*;

В адреса хостов в подсети могут быть *любыми*.

То есть, если наш адрес **192.168.200.47** и маска равна **/20,** то диапазон можно посчитать:

11000000.10101000.11001000.00101111 –адрес

<u>11111111.11111111.11110000.00000000</u> –маска

11000000.10101000.1100XXXX.XXXXXXXX –диапазон адресов

где 0,1 – определенные значения разрядов, X – любое значение,

Что приводит к диапазону адресов:

от **11000000.10101000.11000000.00000000 (192.168.192.0)** до **11000000.10101000.11001111.11111111 (192.168.207.255)**

Следует учитывать, что некоторые адреса являются запрещенными или служебными и их нельзя использовать для адресов хостов или подсетей. Этоадреса, содержащие:

2. **0** в*первом*или*последнем*байте,
3. **255** в*любом*байте (это широковещательные адреса),
4. **127** в*первом*байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня). Поэтому доступный диапазон адресов будет несколько меньше.

Задания для самостоятельного решения:

1. Какие адреса из приведенного ниже списка являются допустимыми адресами хостов:
   0.10.10.10
   10.0.10.10
   10.10.0.10
   10.10.10.10
   127.0.127.127
   127.0.127.0
   255.0.200.1
   1.255.0.0
2. Перечислите все допустимые маски.
3. Определите диапазоны адресов подсетей (даны адрес хоста и маска подсети):
   10.212.157.12/24
   27.31.12.254/31
   192.168.0.217/28
   10.7.14.14/16
4. Какие из адресов
   241.253.169.212
   243.253.169.212

242.252.169.212

242.254.169.212

242.253.168.212

242.253.170.212

242.253.169.211

242.253.169.213

будут достигнуты напрямую с хоста **242.254.169.212/21**

5. Посмотрите параметры IP на своем компьютере с помощью команды **ipconfig.** Определите диапазон адресов и размер подсети, в которой Вы находитесь. Попробуйте объяснить, почему выбраны такие сетевые параметры и какие сетевые параметры выбрали бы Вы.

Вопросы для проверки:

1. Чем занимается сетевой уровень?
2. Что такое сеть передачи данных?
3. Какие требования предъявляются к сетевой адресации?
4. Можно ли использовать в качестве сетевого MAC-адрес?
5. Что такое маска подсети,?
6. Какова структура IP-адреса?
7. Чем определяется размер подсети?
8. Как определить диапазон адресов в подсети?
9. Как определить размер подсети?

Сетевой уровень отвечает за возможность доставки пакетов по сети передачи данных – совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP» означает «набор протоколов, связанных с IP и TCP(протоколом транспортного уровня)».

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи.

Однако предполагается, что каждая подсеть может принять пакет информации

(данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий *шлюз* (шлюз подключен к подсети также как обычный узел). *Шлюз* (gateway)– любое сетевое оборудование с несколькими сетевыми интерфейсами и осуществляющее продвижение пакетов между сетями на уровне протоколов сетевого уровня.

Из шлюза пакет направляется по определенному *маршруту* через систему *шлюзов* и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель; там пакет направляется к получателю.

Таким образом, шлюз выполняет *маршрутизацию* – процедуру нахождения в структуре сети пути достижения получателя (построение пути доставки пакетов).

Если хост подключен к нескольким сетям, он должен иметь несколько сетевых адресов, как минимум столько, сколько каналов к нему подключено.

Маршрутизация производится по *правилам маршрутизации*, сведенным в *таблицумаршрутизации*.

Даже если хост не является шлюзом между подсетями, все равно в нем присутствует таблица маршрутизации, ведь любой хост должен отправлять пакеты напрямую членам своей подсети, через какой-то шлюз другим подсетям и не передавать в сеть пакеты, предназначенные самому себе (заворачивать их по внутренней петле 127.0.0.1).

Таблица маршрутизации имеет следующий вид:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Сетевой адрес - начальный адрес подсети, порядок достижения которой описывает правило.
Маска сети - маска подсети, которую описывает правило.
Адрес шлюза- показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения. Если пакеты будут идти напрямую, то указывается собственный адрес (точнее тот адрес того канала, через который будут передаваться пакеты).

Интерфейс - указывает адрес канала, через который будут передаваться пакеты.

Интерфейс *всегда принадлежит хосту*, на котором находится правило.

Метрика - определяет время, за которое пакет достигнет сети назначения.

Правила применяются в порядке уменьшения масок.

Правила с равными масками применяются в порядке увеличения метрики.

Применение правила заключается в определении, принадлежит ли хост назначения сети, указанной в правиле, и если принадлежит, то пакет отправляется на адрес шлюза через интерфейс.

Рассмотрим вышеприведенную таблицу маршрутизации, пересортировав правила:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Обратите внимание на маску сети в первом правиле. Она описывает подсеть размером в 1 хост с адресом **255.255.255.255** – это *широковещательный* адрес. Пакеты будут посылаться на адрес **192.168.200.47** через интерфейс **192.168.200.47**. Это наш адрес, т.е. пакеты будут отправляться напрямую.

192.168.200.255 255.255.255.255 192.168.200.47 192.168.200.47 30

Опять широковещательный адрес. Смотри предыдущий комментарий.

192.168.200.47 255.255.255.255 127.0.0.1 127.0.0.1 30

Опять такая же маска, но адрес нашего хоста. Отправлять будем через внутреннюю петлю.

192.168.192.0 255.255.240.0 192.168.200.47 192.168.200.47 30

А вот и наша подсеть. Отправляем напрямую.

127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1

Все, что начинается со 127, отправляем через внутреннюю петлю.

224.0.0.0 240.0.0.0 192.168.200.47 192.168.200.47 30

Класс D – отправляем напрямую.

0.0.0.0 0.0.0.0 192.168.200.1 192.168.200.47 30

Самое интересное правило. Маска покрывает ВСЕ возможные адреса! Пакеты отправляются через наш интерфейс на адрес **192.168.200.1**. Правило применяется последним, поэтому его можно озвучить так: по всем адресам, которые не подошли по предыдущим правилам, пакеты отправляем на адрес **192.168.200.1**

Такой адрес обычно имеется в любой сети и называется **шлюзом по**

умолчанию(default gateway). Этот адрес скрывает от хостов и пользователей структуру сети и позволяетупростить таблицы маршрутизации и снять нагрузку с хостов, перенеся маршрутизацию на специально выделенные шлюзы – маршрутизаторы.

Нетрудно догадаться, что все адреса в колонке **Адрес шлюза** должны достигаться напрямую, т.е. входить в нашу подсеть.

Для работы с таблицами маршрутизации в составе ОС имеется программа **route.**

Одной из основных задач, стоящих при проектировании сетей, является распределение по подсетям сетевых адресов из заданного диапазона, т.е. разделение сети на подсети.

При разделении сети на подсети следует учитывать следующие правила:

- размер подсетей должен быть *степенью двойки*
- имеются *запрещенные адреса*
- начальный адрес подсети должен быть *кратен ее размеру.*

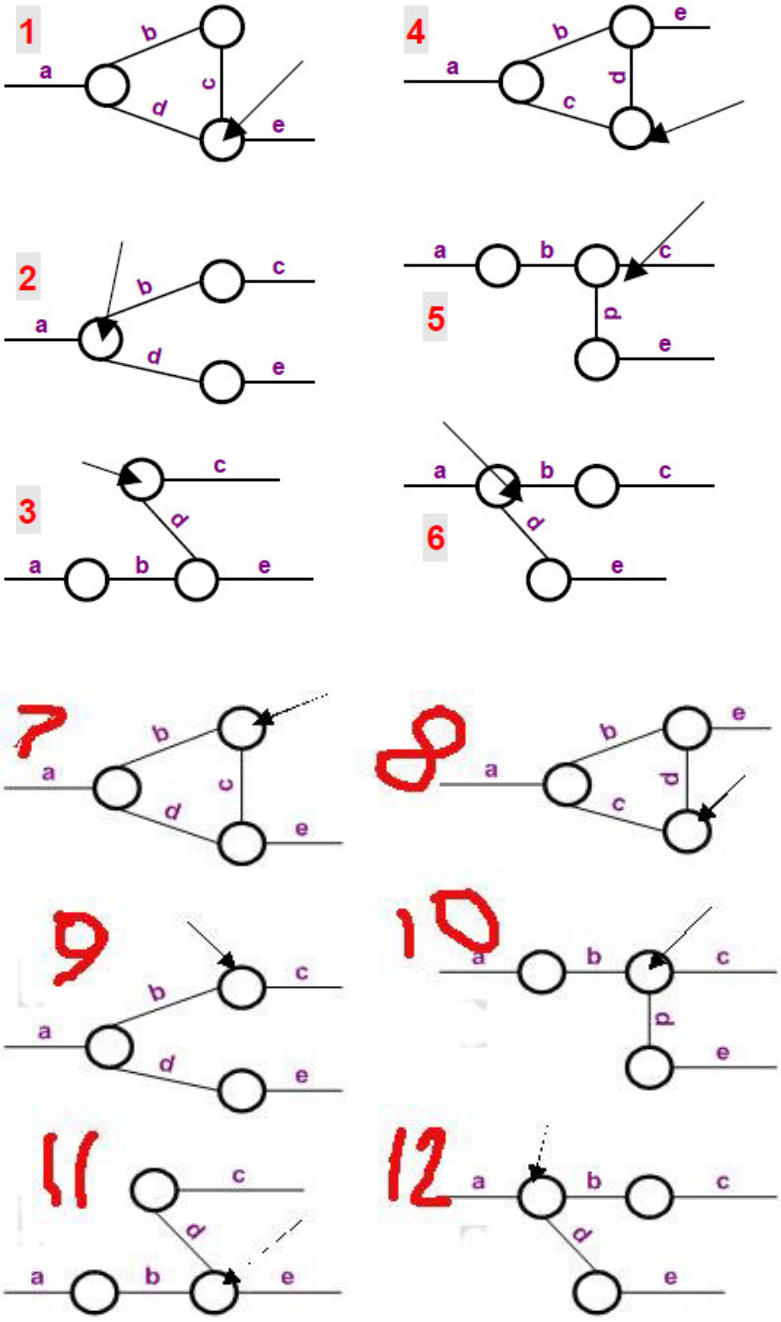
В качестве шлюза по умолчанию можно использовать *любой* узел, но, исходя из увеличения пропускной способности сети и уменьшения времени передачи пакетов, следует в качестве шлюза по умолчанию использовать либо ближайший узел, либо узел, соединенный с максимальным количеством сетей, т.е. следует учитывать *топологию* сети.

Задания для самостоятельного решения:

1. С помощью программы **route print** посмотрите таблицу маршрутизации Вашего компьютера. Объясните все правила.
2. Посмотрите таблицу маршрутизации хоста, имеющего несколько каналов. Объясните все правила.
3. Посмотрите таблицу маршрутизации маршрутизатора. Объясните все правила.
4. Добавьте новое правило в таблицу маршрутизации для сети **192.168.0.0/24** через шлюз в вашей сети с последним байтом в адресе **125** и метрикой **12**
5. Удалите это правило.
6. В соответствии с таблицей и схемами выполните задание на распределение адресов по подсетям (согласно варианта). Постройте таблицы маршрутизации для всех шлюзов и для одного хоста для каждого сегмента.

№ варианта	Количество хостов в подсети					Диапазон адресов	
	a	**b**	**C**	**d**	**e**	**от**	**до**
1	**5**	**10**	**20**	**15**	**50**	**10.0.20.0**	**10.0.20.255**
2	**20**	**15**	**6**	**70**	**25**	**192.168.0.0**	**192.168.0.255**
3	**15**	**25**	**5**	**40**	**5**	**112.38.25.128**	**112.38.25.255**

4	**24**	**32**	**8**	**10**	**2**	**196.13.49.0**	**196.13.49.128**
5	**50**	**16**	**64**	**20**	**15**	**68.76.115.0**	**68.76.115.255**
6	**40**	**6**	**10**	**12**	**5**	**211.3.45.0**	**211.3.45.128**
7	**5**	**10**	**20**	**15**	**50**	**10.0.20.0**	**10.0.20.255**
8	**16**	**12**	**8**	**60**	**20**	**92.190.0.0**	**92.190.0.255**
9	**30**	**15**	**7**	**20**	**8**	**34.40.25.128**	**34.40.25.255**
10	**34**	**22**	**15**	**3**	**2**	**76.17.46.0**	**76.17.46.128**
11	**30**	**26**	**54**	**30**	**15**	**8.71.15.0**	**8.71.15.255**
12	**30**	**16**	**6**	**16**	**5**	**71.5.55.0**	**71.5.55.128**



7. Разделите сеть, состоящую из трех сегментов, имеющую диапазон адресов 192.168.0.32 – 192.168.0.159 на подсети, содержащие 64, 20 и 44 хостов (включая шлюзы).

Вопросы для проверки:

1. Сколько адресов может иметь хост?
2. Может ли у хоста быть прописано несколько шлюзов и почему?
3. Может ли у хоста быть прописано несколько шлюзов по умолчанию и почему?
4. Чем отличаются таблицы у разных классов сетевых устройств и почему?
5. Почему начальный адрес подсети должен быть кратен ее размеру?
6. Чем Вы руководствовались при выборе шлюзов по умолчанию?
7. Может ли физический сегмент сети содержать несколько сетевых подсетей?

2.5 Лабораторная работа № 5 (2 часа)

Тема: «Сетевое оборудование. Параметры и настройка сетевого адаптера»

2.5.1 Цель работы: изучить принцип работы сетевого оборудования. Произвести настройку сетевого адаптера.

2.5.2 Задачи работы:

1. Изучить принцип работы репитера (повторителя);
2. Изучить принцип работы концентратора;
3. Изучить принцип работы моста;
4. Изучить принцип работы коммутатора;
5. Изучить принцип работы маршрутизатора;
6. Изучить принцип работы сетевого адаптера, произвести его настройку.

2.5.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Сетевой адаптер;
2. Репитеры (повторители);
3. Концентраторы;
4. Мосты;
5. Коммутаторы;
6. Маршрутизаторы.

2.5.4 Описание (ход) работы:

Repeaters - Репитеры (поворители)

Сети Ethernet могут быть расширены при использовании устройства, называемого репитер (repeater-повторитель). Репитер Ethernet - это устройство, физически расположеное в сети, с двумя или более Ethernet портами. Эти порты могут быть любого типа: AUI, BNC, RJ-45 или fiber-optic, а также в любой комбинации. Основная функция репитера - получив данные на одном из портов, немедленно перенаправить (forward) их на другие порты. В

процессе передачи данных на другие порты, данные также формируются заново, чтобы исключить любые отклонения, которые могли возникнуть во время движения сигнала от источника. Репитеры так же могут выполнять функцию, называемую "разделение". Если репитер определяет большое количество коллизий, происходящих на одном из портов, он делает вывод, что произошла авария где-то на этом сегменте, и изолирует его от остальной сети. Эта функция была сделана для предотвращения распространения ошибок одного сегмента на всю сеть.

У репитеров имеется отрицательная черта, заключающаяся в том, что он вносит задержку в распространение сигнала по сети. Всесети Ethernet используютпротоколдоступаназываемый CSMA/CD ("Carrier Sense Multiple Access, with Collision Detection"). Чтобы этот протокол работал нормально, ему необходимо иметь возможность определять возникновение коллизии. CSMA/CD определяет это возникновение, сравнивая данные, находящиеся в сети, с тем, что должны были отправить в сеть. Если определяется любое отличие, то это означает, что произошла коллизия (одновременная передача двумя устройствами) и передача немедленно прекращается. CSMA/CD затем ждет случайный отрезок времени и повторяет попытку передачи. Существует изъян в CSMA/CD, который ограничивает размер сети. Посылаемые биты не попадают мгновенно во все точки сети, необходим некоторый небольшой отрезок времени, для того чтобы сигнал прошел по проводам и через каждый репитер в сети. Это время может быть измерено, и оно называется "задержкой распространения" ("Propagation Delay"). Если "задержка распространения" между источником сигнала и наиболее удаленным источником сети больше, чем половина размера наименьшего пакета (frame), который может существовать, тогда CSMA/CD не сможет правильно определить коллизию, и данные в сети могут быть потеряны или искажены.

Согласно проведенным разработчиками Ethernet вычислениям и измерениям, на пути сигнала в сети не может быть более 4-х репитеров и не более 5-ти сегментов, причем только к трем из них могут быть подключены устройства. Эти выводы обычно выражаются в виде правила "5-4-3". Причем, в целом в сети может быть больше 4-х репитеров, но нас интересует только их количество между двумя любыми точками. Существует еще одна формулировка этого же самого правила. В ней в качестве репитера рассматривается связка из двух повторителей и провода между ними. Таких репитеров в сети между любыми двумя компьютерами может быть не более двух

Концентраторы

Концентратор (hub) – это устройство, которое выполняет функции связующего звена для кабеля в сети с топологией «звезда». Каждый компьютер отдельным кабелем подключён к центральному концентратору. Концентратор отвечает за распространение трафика, пришедшего на любой из портов, через все остальные порты. В зависимости от сетевой

среды в устройстве концентратора могут быть применены электрические схемы, оптические компоненты или другие технологии для распределения выходящего сигнала между всеми выходными портами. Концентратор для оптоволокна, например, использует зеркала для того, чтобы расщепить световые импульсы. Внешне концентратор представляет собой коробку, либо стоящую отдельно, либо смонтированною в стойке, с пронумерованными портами, к которым подключается кабель. Порты могут быть: стандартными гнёздами RJ – 45 для сетей на основе витой пары, гнёздами под ST – коннекторы для оптоволоконного кабеля или разъёмами под любые другие виды коннекторов, применяемых в сетях с топологией «звезда». Термин «коннектор» употребляется при описании сетей Ethernet, в сетях Token Ring аналогичное устройство называется модулем множественного доступа (multistation access unit). Внутреннее функционирование этих двух устройств различно, но их основное назначение одно: объединять совокупность компьютеров в единую область коллизий.

Маршрутизаторы

Маршрутизация (routing) и коммутация (switching) являются базовыми концепциями для построения корпоративных сетевых комплексов и формирования инфраструктуры самой большой интерсети – Интернета. Большинство людей представляют себе маршрутизацию как дорогие, специализированные устройства для крупных корпоративных сетей. Во многих случаях это, конечно, совершенно верно, но маршрутизатор может также действовать и в значительно меньших масштабах. Если, например, домашний компьютер используется для связи по телефонной линии с системой, расположенной в офисе, и доступа к ресурсам корпоративной сети, то офисная система функционирует как маршрутизатор. Похожим образом осуществляется соединение систем в ЛВС с Интернетом – компьютер, непосредственно подключённый к Интернету, является маршрутизатором. Маршрутизаторы бывают аппаратными или программными и могут варьироваться от простых моделей до чрезвычайно сложных

Коммутаторы

Коммутатор (или коммутирующий концентратор) по существу представляет собой многопортовое устройство – мост, у которого каждый порт связан с отдельным сегментом сети. Внешне похожий на концентратор, коммутатор принимает входящий трафик через свои порты, но в отличие от концентратора, который передаёт исходящий трафик на всё множество портов, коммутатор направляет трафик только через один порт, необходимый для достижения места назначения. Например, если имеется небольшая сеть рабочей группы, внутри которой каждый компьютер подключён к порту одного коммутирующего концентратора, то каждая система имеет соединение, равнозначное выделенному, с любой другой системой. В этом случае не существует совместно используемой сетевой среды передачи, и, соответственно, нет коллизий или перегруженности трафика.

В качестве дополнительного бонуса, обеспечивается повышенная безопасность, поскольку отсутствие разделяемой среды передачи не позволяет неавторизированным рабочим станциям просматривать и захватывать трафик, не предназначенный им. Замена концентраторов коммутаторами – это превосходный способ увеличить производительность сети без изменения протоколов или модификаций отдельных рабочих станций.

Мост (bridge)

Мост (bridge) - это устройство, которое также используется для соединения сегментов кабеля ЛВС, но в отличие от концентраторов мосты функционируют на Канальном уровне модели OSI и осуществляют отбор передаваемых через них пакетов. Повторители и концентраторы же разработаны для передачи всего получаемого ими трафика во все присоединенные сегменты кабеля. Мост имеет два или более портов, подключенных к различным сегментам кабеля, и работает в беспорядочном режиме (promiiscuous mode), принимая все пакеты, передаваемые по присоединенным сегментам. Для каждого полученного мостом пакета устройство считывает адрес получателя из заголовка протокола Канального уровня, и, если пакет предназначен для системы, расположенной в другом сегменте, передает пакет в этот сегмент. Если пакет послан системе в локальном сегменте, мост отбрасывает его, поскольку данные уже достигли своего места назначения. Описанный процесс называется фильтрацией пакетов (packet filtering). Так же, как концентратор или повторитель, мост не вносит изменений в пакет, каким бы ни было содержание кадра Канального уровня. В результате можно не учитывать протоколы, работающие на Сетевом и вышележащих уровнях, при использовании или установке моста.Работая таким образом, мост уменьшает количество избыточного трафика в сети, так как не пропускает ненужные пакеты. Широковещательные сообщения, пропускаемые во все присоединенные сегменты, делают возможным применение протоколов, которые опираются на широковещание, подобных NetBEUI, без ручной настройки системы. Однако в отличие от повторителей мост не пересылает данные в присоединенные сегменты до тех пор, пока пакет не будет получен целиком. Поэтому две системы в разделенных мостом сегментах могут передавать данные одновременно, не опасаясь возникновения коллизии. Таким образом, сегменты, соединенные мостом, остаются в единой области широковещания, но в разных областях коллизий. Например, если производительность сети сильно упала из-за большого трафика, сеть можно разделить на два сегмента, установив посередине мост. Это позволит удерживать локальный трафик внутри сегментов и пропускать широковещательный и прочий трафик, предназначенный для других сегментов. Мосты так же, как концентраторы, выполняют ретранслирующие функции, давая тем самым возможность увеличить длину кабеля.

Существуют три основных типа мостов:

1)Локальный мост обеспечивает фильтрацию пакетов и ретранслирующие услуги для сетевых сегментов одинакового типа. Такой тип устройств также называется листом MAC-уровня, поскольку данные, обрабатываемые им, поднимаются по стеку протоколов только до уровня управления доступом к среде или подуровня MAC (нижнего из двух подуровней, которые составляют Канальный уровень, второй — это подуровень управления логической связью или подуровень LLC). Это простейший тип моста, так как он не нуждается в наличии перекодировки пакетов и буферизации. Устройство просто передает пакеты через соответствующие порты или отбрасывает их.

2)Преобразующий мост обеспечивает те же функции, что и локальный мост, за исключением того, что он может соединять сегменты с разными скоростями работы или различными протоколами. Например, можно использовать преобразующий мост, чтобы присоединить Ethernet к Token Ring, 10BaseT к 100BaseT или 100BaseTX к 100BaseT4. Для мостов данного типа входящие пакеты поднимаются по стеку протоколов до подуровня MAC, где они лишаются своих заголовков протокола Канального уровня и передаются подуровню LLC. Затем данные инкапсулируются соответствующим протоколом для каждого порта, через который мост будет передавать выходящие пакеты. Указанное преобразование усложняет сам мост (и увеличивает его стоимость) и вносит задержку в передачу данных через весь сетевой комплекс, но остается эффективным решением для объединения отдельных сетей в единую область широковещания.

3)Удаленный мост соединяет сетевые сегменты, расположенные на значительном расстоянии друг от друга, используя соединение глобальной сети, такое как модем или арендованная (выделенная) линия. Соединения глобальной сети обычно медленнее и дороже, чем соединения ЛВС. Мост сохраняет пропускную способность, минимизируя передаваемый через соединение трафик, и в то же время, предоставляя обоим сегментам полный доступ к сети. Из-за разницы в скорости работы локальной и глобальной линий связи удаленный мост обычно имеет внутренний буфер для хранения полученных из ЛВС данных до тех пор, пока они не будут отправлены удаленному узлу сети.

Сетевая карта или сетевой адаптер - это плата расширения, вставляемая в разъем материнской платы (main board) компьютера. Также существуют сетевые адаптеры стандарта PCMCIA для ноутбуков (notebook), они вставляются в специальный разъем в корпусе ноутбука. Или интегрированные на материнской плате компьютера, они подключаются по какой либо локальной шине. Появились Ethernet сетевые картыподключаемые к USB (Universal Serial Bus) порту компьютера.

Сетевые платы характеризуются своей:

- Разрядностью: 8 бит (самые старые), 16 бит и 32 бита. Следует ожидать появления 64 бит сетевых карт (если их уже не выпустили).

- Шиной данных, по которой идет обмен информацией между материнской платой и сетевой картой: ISA, EISA, VL-Bus, PCI и др.
- Микросхемой контроллера или чипом (Chip, chipset) , на котором данная плата изготовлена. И который определяет тип используемого совместимого драйвера и почти все остальное :разрядность, тип шины и т.д.
- Поддерживаемой сетевой средой передачи (network media) , т.е. установленными на карте разъемами для подключения к определенному сетевому кабелю. BNC для сетей на коаксиальном кабеле, rJ45 для сетей на витой паре или разъемы для подключения к волоконной оптике.
- Скоростью работы: Ethernet 10Mbit и/или Fast Ethernet 100Mbit, Gigabit Ethernet 1000Base-T.
- MAC- адресом

Для определения точки назначения пакетов (frames) в сети Ethernet используется MAC-адрес. Это уникальный серийный номер присваиваемый каждому сетевому устройству Ethernet для идентификации его в сети. MAC-адрес присваивается адаптеру его производителем, но может быть изменен с помощью программы. Делать это не рекомендуется (только в случае обнаружения двух устройств в сети с одним MAC- адресом). При работе сетевые адаптеры просматривают весь проходящий сетевой трафик и ищут в каждом пакете свой MAC-адрес. Если таковой находится, то устройсво (адаптер) декодирует этот пакет. Существуют также специальные способы по рассылке пакетов всем устройствам сети одновременно (broadcasting). MAC-адрес имеет длину 6 байт и обычно записывается в шестнадцетиричном виде, например **12:34:56:78:90:AB**

Двоеточия могут и отсутствовать, но их наличие делает число более читаемым. Каждый производитель присваивает адреса из принадлежащего ему диапазона адресов. Первые три байта адреса определяют производителя.

При выборе сетевого адаптера следует принять во внимание следующие соображения.

- Тип шины данных, установленной в вашем компьютере (ISA, VESA, PCI или какой-либо еще). Старые компьютеры 286, 386 содержат только ISA, соответственно и карту вы можете установить только на шине ISA. 486 - ISA и VESA или ISA и PCI (хотя существуют платы поддерживающие все три ISA, VESA и PCI). Узнать это можно посмотрев в описании или посмотрев на саму материнскую плату, после того как откроете корпус компьютера. Вы можете установить сетевую карту в любой соответствующий свободный разъем. Pentium,Pentium Pro, Pentium-2 и им подобные используют ISA и PCI шины данных, причем шина ISA - для совместимости со старыми картами. Есть еще одно достаточно веское соображение - шина ISA,

скорее всего постепенно будет вытеснена шиной PCI. Но произойдет это, наверное, через пару лет, когда ваш адаптер, наверное, дешевле будет сдать в музей.

- Тип сети к которой вы будете подключаться. Если, например, вы будете подключаться к сети на коаксиальном кабеле (10Base-2, "тонкий" Ethernet), то вам нужна сетевая карта с соответствующим разъемом (BNC).
- Его стоимость, учитывая, что цена на самое передовое компьютерное оборудование падает очень быстро. А выйти из строя сетевая карта, при неблагоприятных обстоятельствах, может очень легко вне зависимости от того, сколько денег вы за нее заплатили.
- Еще надо учитывать поддержку вашего адаптера различными операционными системами.

В случае совместимых, например, с NE2000 ISA адаптеров проблем, обычно, не возникает, вы просто указываете "NE2000 Compatible" не задумываясь какая фирма его произвела. Существует еще целый ряд адаптеров, поддержка которых обеспечена практически во всех операционных системах. Для того, чтобы проверить какие сетевые карты поддерживает ваша ОС надо посмотреть в "Compatibility List". Часто в таком списке указан чип, котрый поддерживается, т.е. если приобретаемый сетевой адаптер сделан на основе этой микросхемы, то все будет работать.

Сетевая карта вставляется в соответствующий разъем шины данных, расположенный на материнской плате. Если сетевая карта предназначена для шины данных ISA, то вставлять надо в любой свободный разъем ISA. Если сетевая карта предназначена для шины данных PCI, то вставлять надо в любой свободный разъем PCI.

Разъем ISA - 16bit

Разъем PCI

В компьютере

Для нормальной работы каждой сетевой платы ей необходимы адрес ввода-вывода (In/Out port) и номер прерывания (IrQ).

Конфигурирование сетевой платы заключается в настройке ее на свободные адрес и прерывание, которые затем будут использоваться операционной системой. Адрес (i/o port) и прерывание(IrQ) для каждой сетевой платы должно быть свое, отличное от других устройств компьютера. Современные сетевай карты, поддерживающие технологию Plug-n-play сами выполняют эту операцию, для всех остальных необходимо самим проделать ее.

Порядок настройки сетевой карты зависит от ее модели и конфигурации. Большинство современных сетевых карт поддерживают стандарт Plug-And- Play, и операционная система автоматически обнаруживает эти устройства после их установки и включения питания компьютера: при этом пользователю достаточно лишь указать в соответствующем окне, откуда система должна копировать соответствующие драйверы. Более старые сетевые адаптеры (в основном, подключаемые к шине ISA) не определяются в Windows автоматически и требуют настройки вручную. В ряде случаев на самой плате сетевого адаптера имеется набор перемычек или переключателей, посредством которых можно выставить режим его настройки. Внимательно ознакомьтесь с технической документацией вашей сетевой карты прежде, чем приступить к ее конфигурированию. Однако в некоторых случаях автоматическая настройка Plug-And-Play-адаптеров происходит некорректно, и в результате возникают аппаратные конфликты между сетевой картой и иным оборудованием. Как правило, подобные ситуации бывают вызваны тем, что несколько различных устройств начинают несанкционированно использовать одни и те же ресурсы, например запрос на прерывание (IRQ,Interrupt Request), адреса каналов непосредственного доступа к памяти (DMA, Direct Memory Access) или диапазон ввода-вывода (I/O Range). Решить эту проблему можно одним из перечисленных ниже способов.

1. Во время перезагрузки компьютера войдите в настройки BIOS, перейдите в раздел конфигурации шины PCI или ISA, позволяющий изменить назначенные различным слотам этих шин аппаратные прерывания, и освободите одно из прерываний для соответствующей шины, которое будет впоследствии автоматически назначено сетевому адаптеру. Например, если известно, что ваш сетевой адаптер, подключенный к слотуPCI,требует прерывание 20, назначьте для одного из слотов шины PCI зна- чение IRQ = 20. Если это не помогло, можно поступить так, как показано в следующем пункте.

2. Переместив на плате сетевого адаптера соответствующую перемычку или переключатель либо воспользовавшись программой-конфигуратором сетевого адаптера, отключите режим Plug-And-Play для сетевой карты. Далее ее можно настроить как аппаратно-конфигурируемое или программно-конфигурируемое устройство.

Настройка сетевого адаптера

Далее требуется удостовериться, что сетевая карта правильно опозналась системой Windows и работает нормально. Для этого откройте панель упраления Windows, как показано ниже, и выберите там пиктограмму "Система"

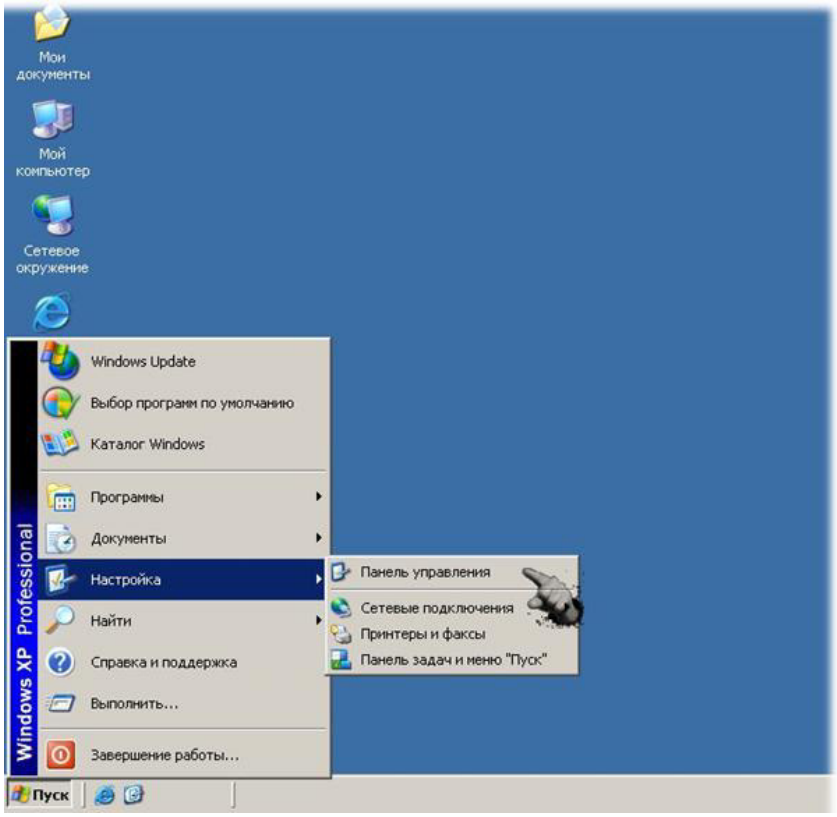


Рисунок 1. Открытие панели управления

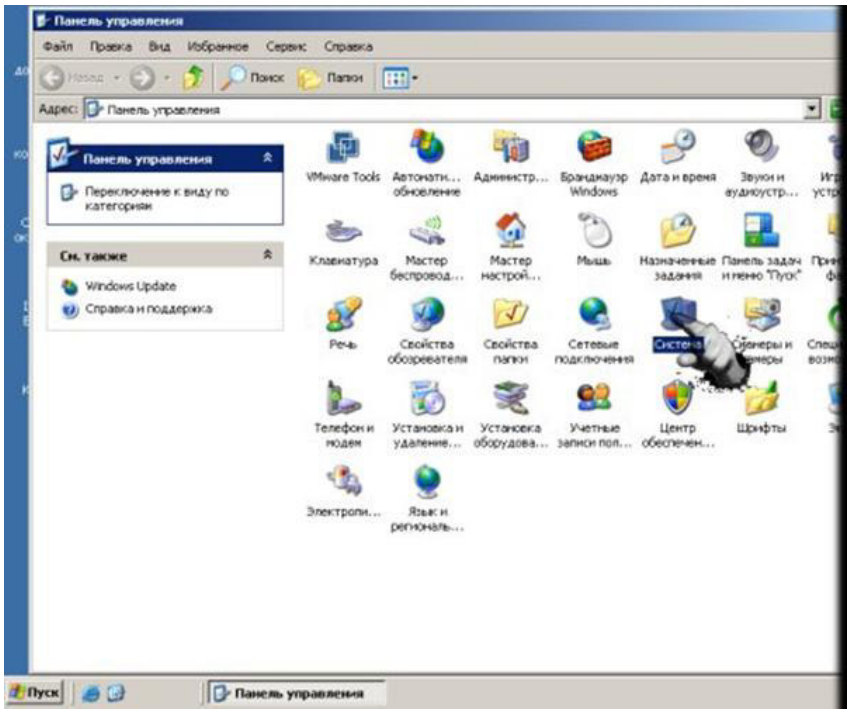


Рисунок 2. Панель управления

В открывшемся окне выбирается вкладка "Оборудование" , далее в следующем окне "Диспетчер устройств".

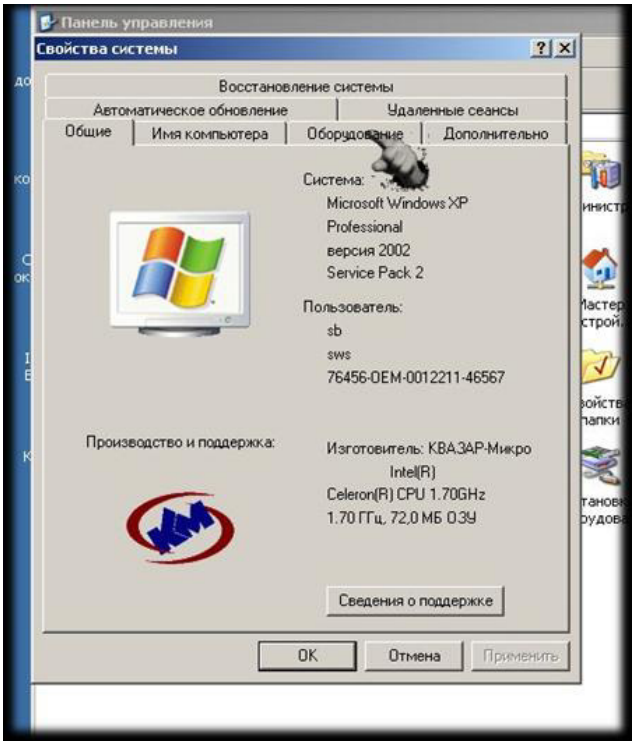


Рисунок 3. Свойства системы

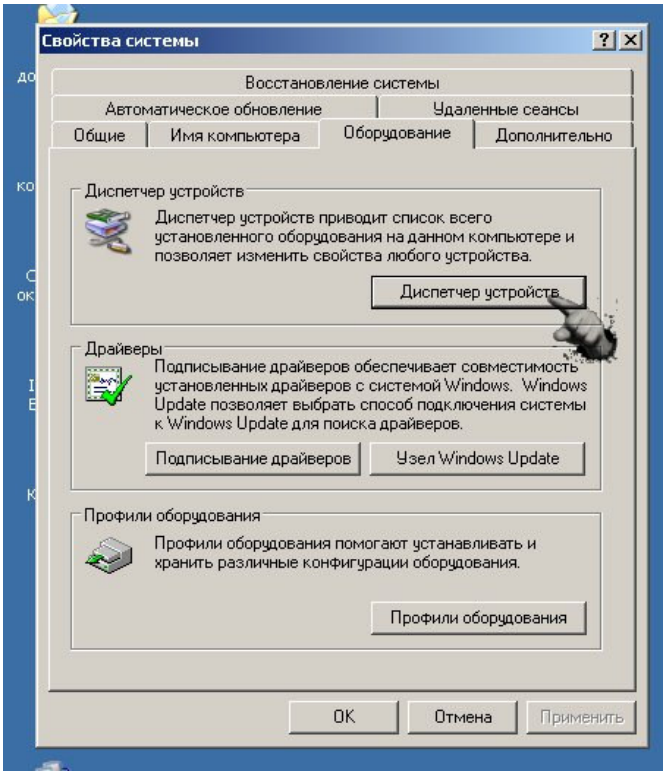


Рисунок 4. Свойства системы вкладка оборудование.

В дереве "Диспетчера устройств" должен присутствовать раздел "Сетевые платы", в котором должна быть представлена установленная сетевая карта.

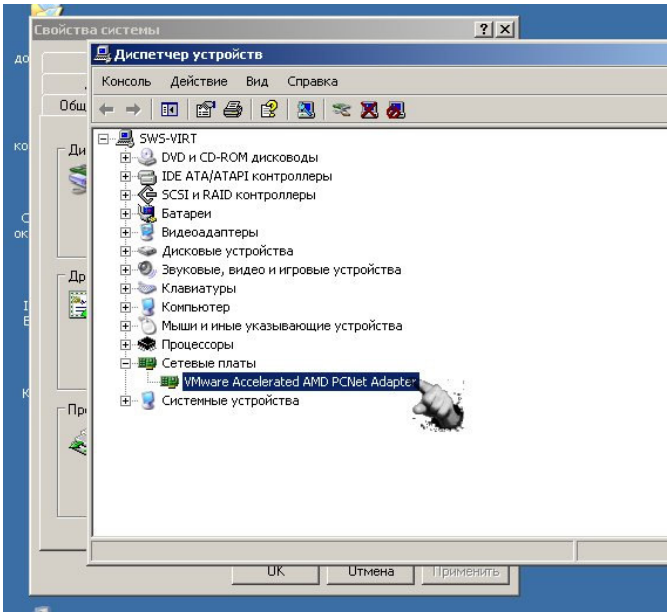


Рисунок 5. Диспетчер устройств

Если отсутствует соответствующий раздел, или расцвечен вопросительными/восклицательными знаками, что есть признак некорректной установки платы, обращайтесь к пооставщику компьютера или своему гуру-самоделкину.

По двойному щелчку на соответствующем устройстве (сетевой плате) в следующем окне в основном поле если все в порядке, сможете прочитать "Устройство работает нормально"

Обратите также внимание - в выпадающем списке "Применение устройства" (ниже поля состояния устройства) должно стоять:
"Это устройство используется(включено)"

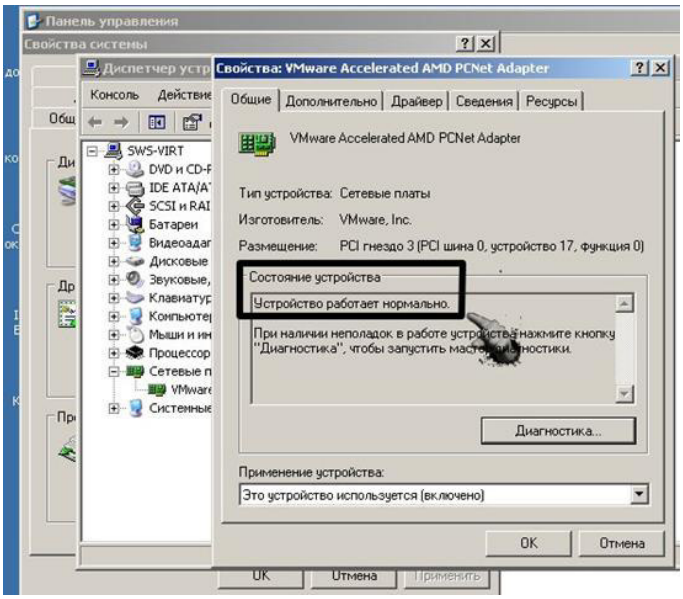


Рисунок 6. Свойства сетевой платы

Дополнительным критерием работоспособности есть установленные на некоторых сетевых платах индикаторы. При подключенном кабеле они неупорядоченно мерцают

"Настройка локальной сети в WinXP "

- Реализация прямого соединения
- Папка "Сетевое окружение"
- Настройка первичного (LAN) сетевого соединения в Windows XP

Реализация прямого соединения

Самая простая с точки зрения технической реализации возможность установления связи между двумя компьютерами - *прямое соединение* (peer-to-peer) по последовательным или параллельным портам. Встороеннаяфункция операционной системы windows (начиная с версии 95) позволяет легко установливать прямое соединение компьютеров.

Пошаговая процедура установки прямого соединения:

- Проверьте возможность доступа извне к ресурсам вашего компьютера. Для этого выполните следующие действия: откройте **Панель управления** -> **Сетевые подключения** -> **Свойства** -> **Служба доступа к файлам и принтерам** и активизируйте нужную опцию.
- Определите доступ к каким файлам и папкам должен иметь подключенный компьютер.
- Выключите оба компьютера и присоедините кабель к соответствующим портам на задней стенке системного блока, после этого включите компьютеры
- Далее запустите программу прямого соединения нажав на кнопку **Пуск** и выбрав последовательно пункты меню: **Программы** -> **Стандартные** -> **Связь** ->**Мастер новых подключений**-> **Установить прямое подключение к другому компьютеру**->**Подключиться напрямую к другому компьютеру**.

  Если пункт меню *Прямое соединение* отсутсвует, то выполните его установку, с помощью *Панели управления*
- В появившемся окне определите статус вашего компьютера:

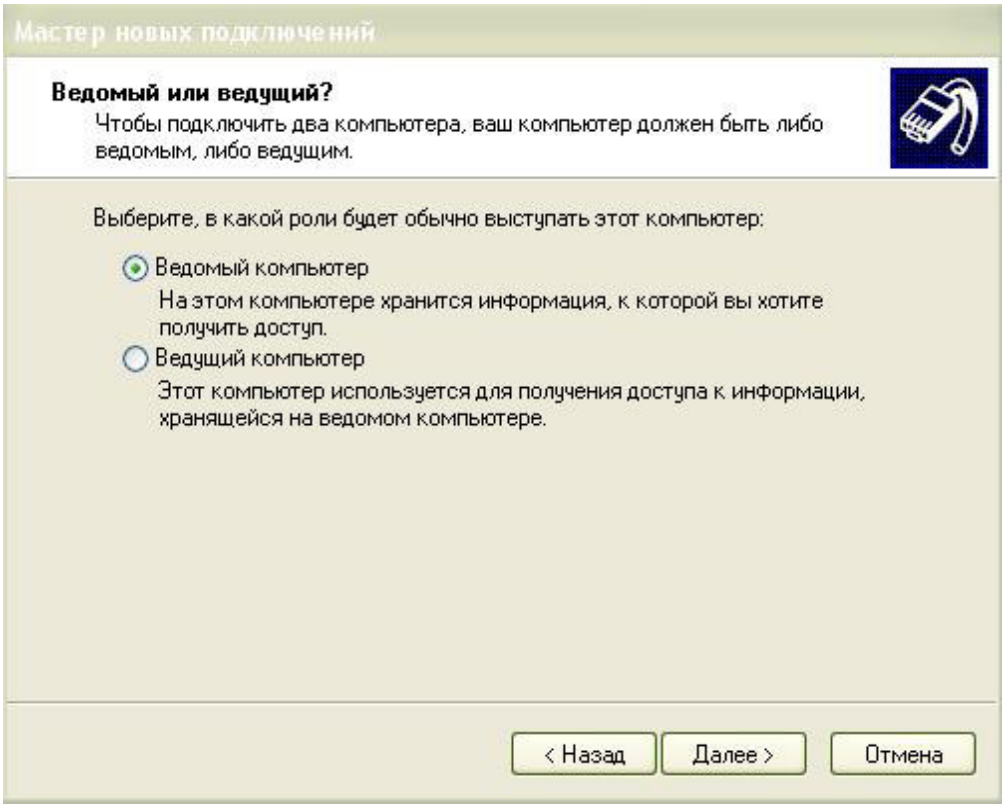


Рисунок 7. Мастер новых подключений

Ведомый

Компьютер, на котором находятся необходимые данные

Ведущий

Компьютер, осуществляющий доступ к ресурсам ведомого компьютера

Выберите **Ведущий**

Определив статус компьютера, нажмите кнопку **Далее** для открытия следующего диалогового окна - окна выбора порта соединения

Рисунок 8. Мастер новых подключений

Выбрав нужный порт нажимайте кнопку **Далее**, откроется следующее диалоговое окно.

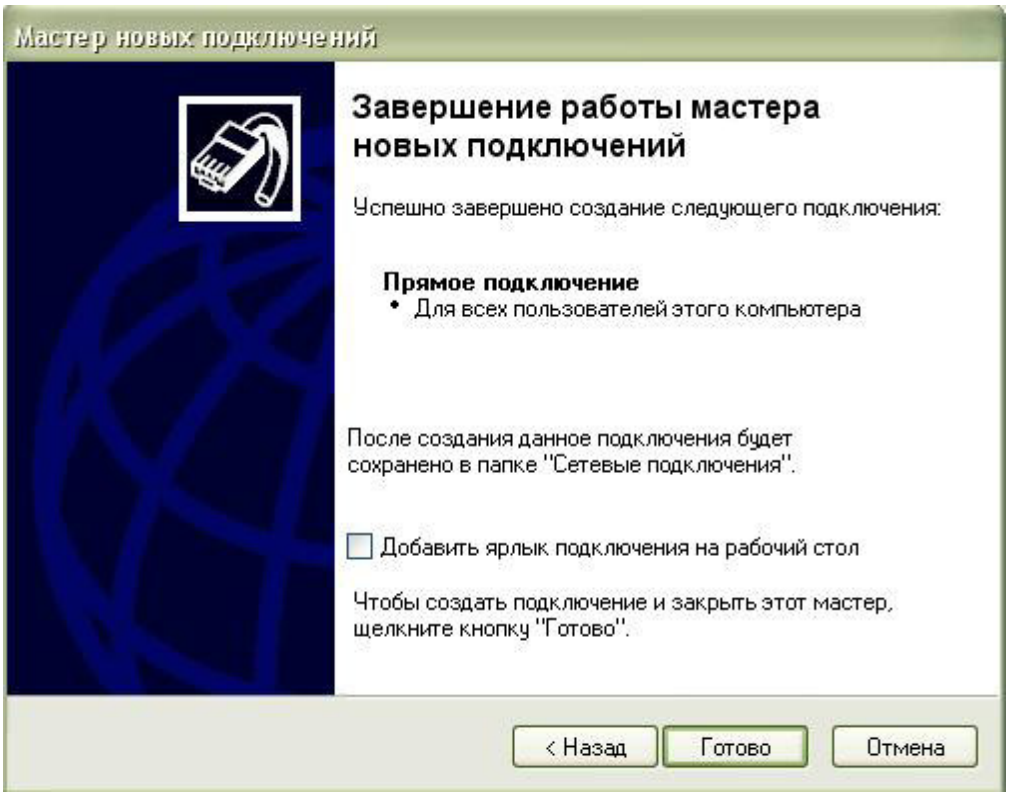


Рисунок 9. Мастер новых подключений

Прежде чем нажать кнопку **Готово**, проведите установку прямого соединения на ведомом компьютере. Она происходит аналогично вышеописанной процедуре, только теперь в первом диалоговом окне выберите пункт **Ведомый**

Запустите прямое соединение, нажав кнопку **Готово** на ведущем компьютере. Сначала на ведомом, а затем и на ведущем появится следующее окно:

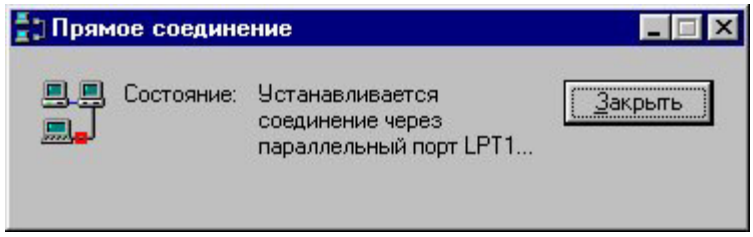


Рисунок 10. Установка соединения

При соединении со стороны ведущего компьютера укажите имя ведомого. Теперь вы получили доступ к ведомому компьютеру и хранящимся на нем данным.

Папка "Мое сетевое окружение"

Папка "Сетевое окружение" предназначена для организации работы в сети.

Обычно на рабочем столе windows находится значок "Сетевое окружение", позоляющий открыть папку "Сетевое окружение" В папке "Сетевое окружение" по умолчанию отображается информация о "своей" рабочей группе.

Свойства папки "Сетевое окружение" позволяют настроить компьютер для работы в сети

Настройка первичного (LAN) сетевого соединения в Windows XP

На этом этапе вам потребуется знать, какой IP-адрес выделен компьютеру и адрес сервера DNS.

Допустим, вам выдан адрес 192.168.68.30

Адрес DNS сервера 192.168.68.1

По аналогии, если выдан адрес 192.168.64.30 (или 192.168.64.199, скажем), то адрес DNS сервера будет 192.168.64.1

Сетевая маска в любом случае 255.255.255.0

Переходим в "Панель управления" и выбираем "Сетевые подключения"

Здесь возможен вариант, когда настроенных подключений нет, тогда выбираете "Создание нового подключения" и далее следуете за Мастером создания подключения , либо вариант, когда подключение по локальной сети существует, но работает неправильно, выбираете пункт "Изменение настроек подключения"

При этом откроется следующее окно, выбирайте в нем пункт "Протокол Интернета(TCPIP)", нажмите на кнопку "Свойства"

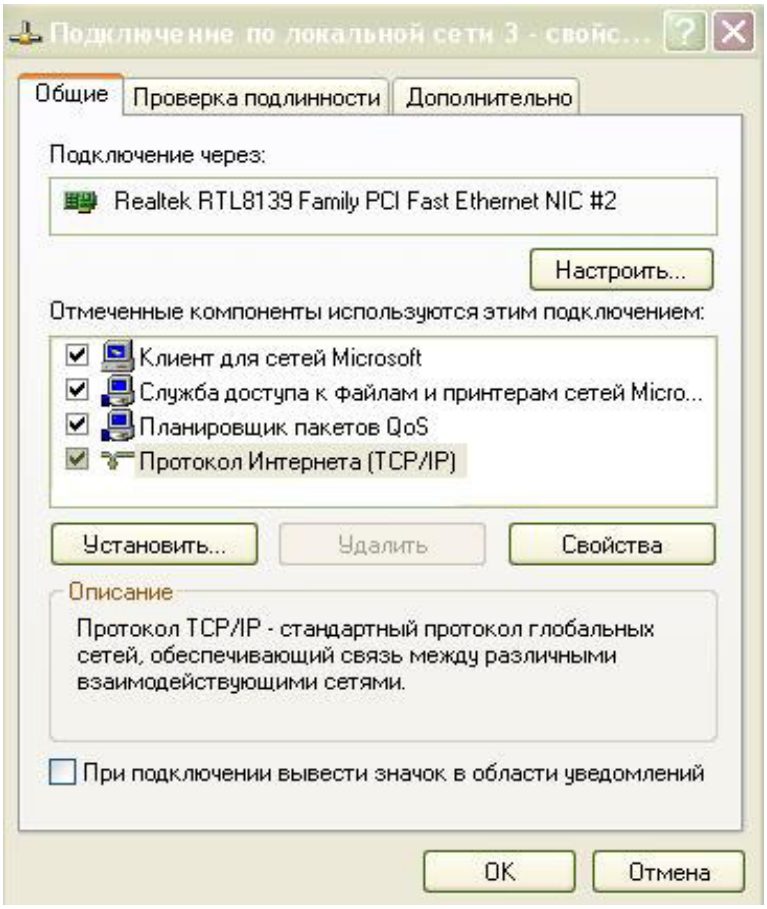


Рисунок 11. Подключение по локальной сети

Здесь на главной странице заполняем форму в соответствии с входными данными:

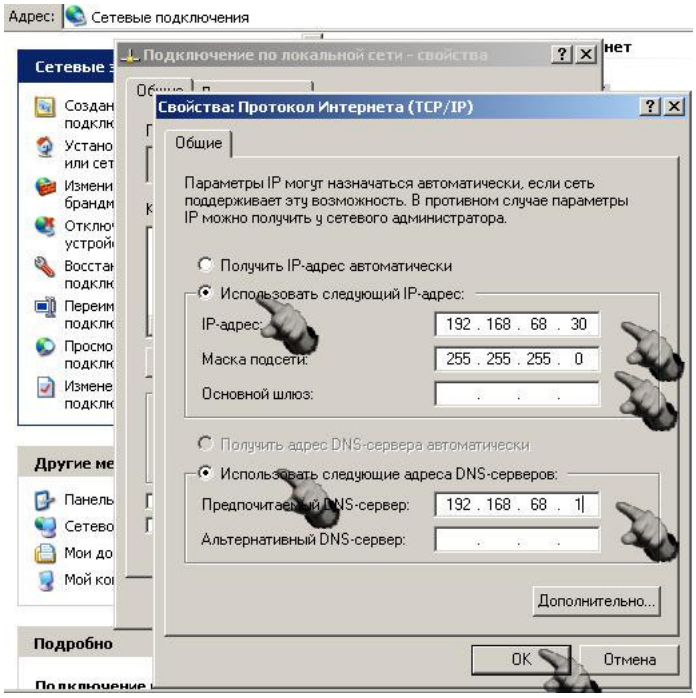


Рисунок 12. Свойства протокол интернете TCP/IP

Больше ничего по данному протоколу заполнять не нужно!

Вернувшись в "Свойства подключения по локальной сети", можете включить/выключить "Клиент для сетей Microsoft" и "Службу доступа к файлам и принтерам сети Microsoft" по своему усмотрению. Эти пункты никак не влияют на подключение к Интернет. С их помощью вы можете участвовать, являясь участником рабочей группы сети Windows, в файлообмене с другими компьютерами в своем доме/районе и открывать доступ к своим файлам.

Равно как и своим вирусам и участвовать в вирусообмене. Поэтому хозяин-барин. Если же вы на это решились, установите имя компьютера и рабочую группу Windows, выбрав "Система" в Панели управления Windows, а там вкладку "Имя компьютера", как показано ниже:

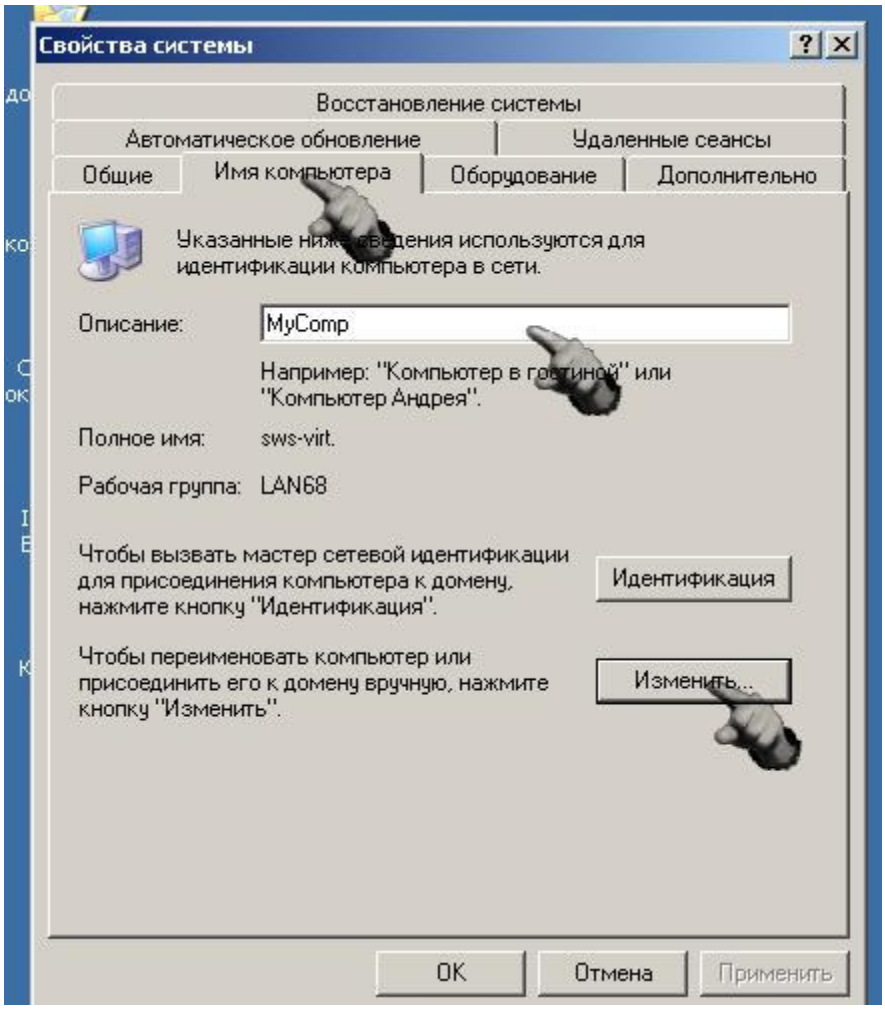


Рисунок 13. Свойства системы.

Рекомендованное имя рабочей группы - LAN68. Не пытайтесь присоединить компьютер к домену или вызвать мастер сетевой идентификации. После всех вышеприведенных действий требуется перегрузить компьютер, если Windows об этом еще не просила.

2.6 Лабораторная работа № 6 (2 часа)

Тема: «Протоколы и алгоритмы маршрутизации»

2.6.1 Цель работы: получить сведения о маршрутизации и научиться добавлять маршруты в таблицу маршрутизации.

2.6.2 Задачи работы:

1. Научиться работать с таблицей маршрутизацией.

2.6.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Аппаратные: компьютер с установленной ОС Windows.
2. Программные: Приложения ВМ: VirtualBox; Виртуальные машины: VM-1.

2.6.4 Описание (ход) работы:

В сетях, основанных на протоколе IP, *концепция маршрутизации* является одной из важных. Она создает или разбивает сеть. Неправильная конфигурация маршрутизации способна вывести из строя сеть.

Маршрутизация – технология определения пути доставки (маршрута) пакетов. Основные принципы маршрутизации:

1. Каждая операционная система, поддерживающая стек **TCP/IP**, имеет маршрутизатор и таблицу маршрутизации.
2. Таблица маршрутизации используется только тогда, когда определяется, как доставлять пакеты.
3. Маршрутизация должна быть сконфигурирована корректно на обоих концах связи и на каждом участке между ними.

Для определения пути доставки пакета используется *таблица маршрутизации*. Пример таблицы маршрутизации можно получить командой **route** с параметром *print*.

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.4.1	192.168.4.7	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.4.0	255.255.255.0	192.168.4.7	192.168.4.7	1
192.168.4.7	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.4.255	255.255.255.255	192.168.4.7	192.168.4.7	1
224.0.0.0	224.0.0.0	192.168.4.7	192.168.4.7	1
255.255.255.255	255.255.255.255	192.168.4.7	192.168.4.7	1
Основной шлюз:	192.168.1.1			

Рисунок 1. Пример таблицы маршрутизации

В общем случае для маршрутизации используется следующий *алгоритм*. Из пакета извлекается IP-адрес назначения пакета и производится попытка сопоставить его с адресом назначения (*Сетевой адрес*) каждого элемента таблицы маршрутизации пока не найдется наилучшее совпадение. Если совпадений не найдено, то пакет удаляется и отправителю пакета может отправиться сообщение об ошибке. Сравнение производится с тремя порциями информации: **Сетевой адрес (*Network Destination*), Маска сети (*Netmask*) и IP-адрес назначения пакета.**

В основном, производится побитная операция **AND** между **IP-адресом получателя** и **Маской сетии (*Netmask*)**: если полученное значение равно **Сетевому адресу (*Network Destination*)**, то считается, что совпадение найдено.

Пример 1. Необходимо проверить почту на сервере, чей адрес **192.168.4.100** (используется таблица маршрутизации приведенная ранее). Необходимо выполнить побитную операцию **AND** над **IP-адресом получателя пакетов** и **сетевыми масками (*Netmask*)** из таблицы маршрутизации. Эта операция производится над всем масками из таблицы маршрутизации. Но в рассматриваемом примере только 3-я строка наиболее походит.

	1-й октет								2-й октет								3-й октет								4-й октет							
биты	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ID-сети																													ID-узла		
IP-адрес	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	1	0	0
десятичная запись	192								168								4								100							
Маска	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
десятичная запись	255								255								255								0							
Результат операции AND	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
десятичная запись	192								168								4								0							

Рисунок 2. Пример определения маршрута доставки пакетов

Как видно из приведенной таблицы, результат побитной операции **AND** совпадает с 3-й строкой таблицы маршрутизации (Рисунок 2). Следовательно, пакет отправится по указанному маршруту через интерфейс**192.168.4.7**.

Следует отметить, что указанный в примере IP-адрес после выполнения побитной операции **AND** над масками совпадет больше чем с одной строкой маршрутизации. Для избежания таких случаев используется*приоритет маршрутов*. Система ищет более точное совпадение адреса с маской (255.255.255.255 более точна, чем 255.255.255.0, которая в свою очередь, более точна, чем 0.0.0.0). Маршрут с сетевым адресом 0.0.0.0 и маской 0.0.0.0

является *маршрутом по умолчанию*. Так как этот маршрут подходит к любому адресу назначения, он описывает маршрут, который используется, если не найден более подходящий. Обычно этот маршрут используется для пересылки пакетов провайдеру Интернет-услуг, при подключении к Интернету.

Для работы с таблицей маршрутизации используется стандартная утилита **ROUTE**, которая выводит на экран и изменяет записи в локальной таблице IP-маршрутизации.

Запущенная без параметров, команда **route** выводит справку.

Параметр	**Описание**
add	Добавление маршрута
change	Изменение существующего маршрута
delete	Удаление маршрута или маршрутов
print	Печать маршрута или маршрутов

*Таблица 1. Назначение параметров команды **route***

Пример 2. Добавление маршрута.

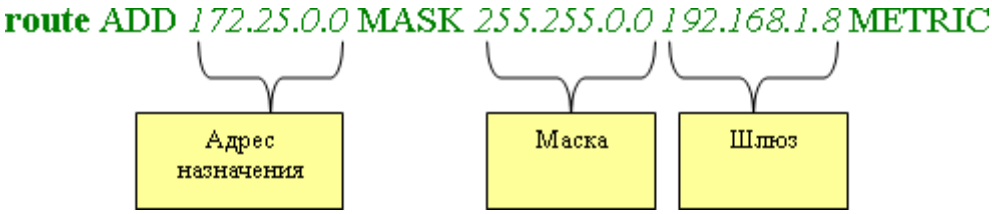


Рисунок 3. СТрока длядобавление маршрута

Задание 1. Создайте таблицу для облегчения определения маршрутов.

1. Откройте **табличный процессор** и сформируйте таблицу по следующему шаблону:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
1		7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
2	**IP-адрес**	192								168								252								56							
3	двоичная запись	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1	1	0	0	0
4	**Маска**	255								255								255								7							
5	двоичная запись	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1
6	**Операция AND**	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
7	**Адрес назначения**																																

Рисунок 4. Образец оформления таблицы

2. Введите в диапазон ячеек **Z3:AG3** формулы для перевода числа в десятичной системе счисления из ячейки **Z2** в двоичную форму (в соответствии с таблицей).

Таблица 2. Формулы для перевода в двоичную систему счисления

Имя Ячейки	**Формула**
AG3	=Z2-2*INT(Z2/2)

AF3	=INT(Z2/2)-2*INT(INT(Z2/2)/2)
AE3	=INT(INT(Z2/2)/2)-2*INT(INT(INT(Z2/2)/2)/2)
AD3	=INT(INT(INT(Z2/2)/2)/2)-2*INT(INT(INT(INT(Z2/2)/2)/2)/2)
AC3	=INT(INT(INT(INT(Z2/2)/2)/2)/2)-2*INT(INT(INT(INT(INT(Z2/2)/2)/2)/2)/2)
AB3	=INT(INT(INT(INT(INT(Z2/2)/2)/2)/2)/2)- 2*INT(INT(INT(INT(INT(INT(Z2/2)/2)/2)/2)/2)/2)
AA3	=INT(INT(INT(INT(INT(INT(Z2/2)/2)/2)/2)/2)/2)- 2*INT(INT(INT(INT(INT(INT(INT(Z2/2)/2)/2)/2)/2)/2)/2)
Z3	=INT(INT(INT(INT(INT(INT(INT(Z2/2)/2)/2)/2)/2)/2)/2)

3. Аналогично введите формулы для преобразования чисел из десятичной системы счисления в двоичную для ячеек **R2,J2,B2**.
4. Аналогично введите формулы для преобразования маски подсети в двоичную систему счисления.
5. Введите формулы для побитной операции **AND** над **IP-адресом** и **маской (*Netmask*)**:
   - введите в ячейку **AG6** формулу **=AND(AG3;AG5)**;
   - скопируйте введенную формулу в диапазон ячеек **B6:AF6**.
6. Введите в ячейку **Z7** формулу для преобразования 4-го октета маски в десятичную систему счисления - **=AG6*2^AL1+AF6*2^AF1+AE6*2^AE1+AD6*2^AD1+AC6*2^AC1+AB6*2^AB1+AA6*2^AA1+Z6*2^Z1**.
7. Аналогично введите формулы для ячеек **R7, J7, B8**.
8. Сохраните файл в своем каталоге с именем ***ROUTE***.

Задание 2. Создайте новый маршрут для вашего компьютера и проследите его.

1. Запустите виртуальную машину **VM-1** и загрузите ОС **Windows**.
2. Откройте **консоль (*Пуск/Программы/Стандартные/Командная строка*)**.
3. Определите IP-адрес вашего компьютера с помощью утилиты **ipconfig**.
4. Просмотрите таблицу маршрутизации на вашем компьютере:

- выведите справку по команде **route** (для этого необходимо ввести команду и нажать клавишу ***ENTER***);

```
Route
```

- выведите таблицу маршрутизации командой **route** с параметром *PRINT*:

```
route PRINT
```

- запомните маршрут по умолчанию (первая строка).

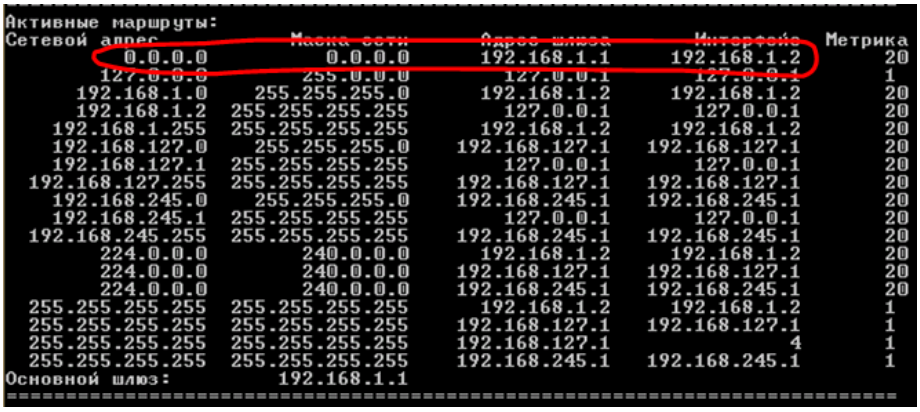


Рисунок 5.Пример вывода программы **ROUTE**

5. Проследите работу маршрутизатора с помощью утилиты *TRACERT*, отправив пакеты на узел **www.opennet.ru**. Введите: tracert www.opennet.ru

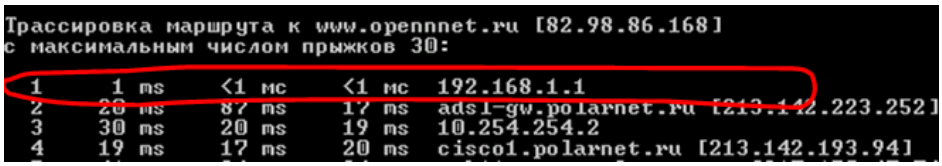


Рисунок 6. Пример вывода программы **TRACERT**

6. *Следует отметить, что пакеты на указанный сайт отправляются через один шлюз (**192.168.1.1**), который видно в первых строках вывода программ **ROUTE** и **TRACERT**.*
7. Добавьте в таблицу маршрутизации компьютера строку для пересылки пакетов в сеть **172.21.0.0** (маска **255.255.0.0**) через сетевой интерфейс компьютера. Введите:

```
route add 172.21.0.0 mask 255.255.0.0 192.168.1.4 METRIC 3
```

8. Проверьте работу внесенных вами изменений с помощью утилиты *TRACERT*.

Самостоятельные задания.

1. Сформируйте маски подсети таким образом, чтобы получались сети, в которых количество уникальных адресов составляют 256, 2048, 32768.

2. Определите маршруты для пакетов в соответствии с таблицей маршрутизации, приведенной в теоретической части лабораторной работы. Результат оформите в виде таблицы и сохраните в своей папке.

Таблица маршрутизации		
IP-адреса пакетов	Адрес шлюза	Интерфейс
10.1.1.1		
192.168.4.121		
127.13.13.210		
192.168.5.121		

2.7 Лабораторная работа № 7 (2 часа)

Тема: «Протоколы TCP/IP»

2.7.1 Цель работы: изучить эталонную модель протоколов ISO/OSI и стек протоколов TCP/IP. Изучить IP-адресацию и правила назначения IP-адресов. Познакомиться с протоколом IP, IP-адресацией, IP-маршрутизацией, протоколом TCP, функциями протокола TCP.

2.7.2 Задачи работы:

1. Изучить эталонную модель протоколов ISO/OSI и стек протоколов TCP/IP;
2. Изучить IP-адресацию и правила назначения IP-адресов.

2.7.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.7.4 Описание (ход) работы:

Протокол – это набор правил, описывающих метод передачи информации по сети. Понятие протокола является исключительно важным для компьютерных сетей. Это связано с тем, что сеть может объединять компьютеры разных типов, работающие под управлением разных операционных систем. Чтобы эти компьютеры могли обмениваться друг с другом информацией, они должны «разговаривать на одном языке», то есть использовать одни и те же протоколы - правила передачи информации по сети.

Стек протоколов TCP/IP является протокольной основой Интернет. Ключевым моментом при этом является IP-адресация.

IP-адрес – это уникальный числовой адрес, однозначно идентифицирующий узел, группу узлов или сеть. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел (так называемых «октетов»), разделенных точками, каждое из которых может принимать значения в диапазоне от 0 до 255, например:

128.10.2.30 - традиционная десятичная форма представления адреса,

10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127

зарезервирован для специальных целей). В сетях класса A количество узлов должно быть больше 2^{16}, но не превышать 2^{24}.

- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 2^8 - 2^{16}. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 2^8. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Класс	Наименьший адрес	Наибольший адрес
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

- если IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;

0 0 0 0 ..... 0 0 0 0

- если в поле номера сети стоят 0, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;

0 0 0 0 .....0 Номер узла

- если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);

1 1 1 1 .....1 1

- если в поле адреса назначения стоят сплошные 1, то пакет, имеющий такой адрес рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);

Номер сети 1111.....11

- адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

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

1. Ознакомиться с теоретическими сведениями по теме. Особенно внимательно изучить материал, относящийся к IP-адресации.
2. На основе примера, разобранного для сетей класса А, заполнить третью колонку таблицы 1.
3. Выполнить аналогичные расчеты и заполнить четвертую и пятую колонки таблицы 1.

Для выполнения задания 2 необходимо выполнить следующие действия:

1. Перевести каждое число IP-адреса в двоичную форму. Для перевода можно воспользоваться программой «Калькулятор», установив «Вид/Инженерный».
2. По первым битам IP-адреса определить класс сети.
3. В соответствии с классом определить маску сети по умолчанию.
4. Выписать только те биты IP-адреса, которые соответствуют единичным битам в маске сети. Представить эти биты в точечной нотации. Это будет номер сети.
5. Выписать те биты IP-адреса, которые соответствуют нулевым битам в маске сети. Представить их в точечной нотации. Это будет номер хоста.
6. В двоичном представлении IP-адреса биты, соответствующие номеру хоста, заменить единицами. Представить получившийся адрес в точечной нотации. Это будет широковещательный адрес.

Задание

1. Ознакомьтесь с теоретическими сведениями по теме «Протоколы. IP-адресация».
2. Заполните таблицу 1 «Характеристики сетей различных классов».

Таблица 1

Номер по порядку	Характеристика сети	Класс сети		
		A	B	C
1	2	3	4	5
1.	Формат первого байта IP-адреса			
2.	Число байтов для номера сети			
3.	Число байтов для номера хоста			
4.	Минимальный номер сети в точечной нотации			
5.	Максимальный номер сети в точечной нотации			
6.	Число различных сетей			
7.	Минимальный номер хоста в точечной нотации			
8.	Максимальный номер хоста в точечной нотации			
9.	Число различных хостов			
10.	Маска сети по умолчанию			

3. Для IP-адреса, указанного в индивидуальном задании, считая, что маска сети задана по умолчанию, определите:
    3.1. Класс сети;
    3.2. Число сетей;
    3.3. Маску сети по умолчанию;
    3.4. Номер сети;
    3.5. Номер хоста;
    3.6. Минимальный номер сети;
    3.7. Максимальный номер сети;
    3.8. Широковещательный адрес.
4. Используя маску, указанную в индивидуальном задании, определите
    4.1. Маску сети (в десятичной нотации);
    4.2. Номер сети (в десятичной нотации);
    4.3. Номер хоста (в десятичной нотации);
    4.4. Минимальный номер хоста;
    4.5. Максимальный номер хоста;
    4.6. Широковещательный адрес;
    4.7. Число хостов.

Пример выполнения задания 2.

Пусть IP-адрес 64.10.20.30

Переводим числа в двоичный формат:

$64_{10}=01000000_2$

$10_{10}=00001010_2$

$20_{10}=00010100_2$

$30_{10}=00011110_2$

Записываем двоичную форму представления IP-адреса:

01000000.00001010.00010100.00011110

Первые биты адреса – 01, значит, это сеть класса А.

Маска сети по умолчанию: 255.0.0.0

Записываем в двоичной форме маску сети и IP-адрес:

Маска: 11111111. 00000000.00000000.00000000

IP-адрес: 01000000. 00001010.00010100.00011110

Эти биты соответствуют номеру сети

А эти биты соответствуют номеру хоста

Значит, номер сети - 01000000_2 или 64_{10}

номер хоста - $00001010.00010100.00011110_2$ или $10.20.30_{10}$

Заменяем в IP-адресе номер хоста единицами, получим широковещательный адрес $01000000.111111.111111.111111_2$ или 64.255.255.255

Следовательно:

IP-адрес	64.10.20.30
Класс сети	A
Маска сети	255.0.0.0
Номер сети	64.0.0.0
Номер хоста	0.10.20.30
Широковещательный адрес	64.255.255.255
Число сетей	2^7-2 =

При выполнении задания 3 необходимо вначале определить маску сети. Маска содержит столько единичных битов, сколько указано в числе после дробной черты. Остальные вычисления выполняются подобно заданию 2.

Контрольные вопросы

- Что такое протокол?
- Назовите уровни модели протоколов модели ISO/OSI и назначение протоколов каждого уровня.
- Назовите уровни стека протоколов TCP/IP и назначение протоколов каждого уровня.
- Приведите примеры протоколов, входящих в стек TCP/IP.

- Что такое аппаратный адрес?
- Что такое IP-адрес?
- Каковы правила назначения IP-адресов?
- Как проанализировать IP-адрес?

Варианты индивидуальных заданий

Таблица 2

Номер варианта	IP-адрес к заданию 3	IP-адрес к заданию 4
1.	192.168.72.33	192.168.72.33/20
2.	190.172.55.40	190.172.55.40/25
3.	123.232.14.72	123.232.14.72/18
4.	196.232.66.54	196.232.66.54/25
5.	193.123.55.67	193.123.55.67/26
6.	191.172.55.42	191.172.55.42/27
7.	178.66.57.18	178.66.57.18/20
8.	10.0.0.20	10.0.0.20/12
9.	67.192.44.89	67.192.44.89/12
10.	128.34.67.11	128.34.67.11/18
11.	193.34.126.44	193.34.126.44/26
12.	156.32.11.93	156.32.11.93/23
13.	167.168.169.170	167.168.169.17/20
14.	145.44.11.77	145.44.11.77/22
15.	132.45.171.99	132.45.171.99/25
16.	198.164.55.55	198.164.55.55/26
17.	192.77.121.144	192.77.121.144/25
18.	12.13.14.15	12.13.14.15/18
19.	44.57.62.39	44.57.62.39/18
20.	152.15.66.5	152.15.66.5/26
21.	132.45.171.99	132.45.171.99/27
22.	198.164.155. 5	198.164.155.5/26
23.	192.77.11.44	192.77.11.44/29
24.	12.130.140.150	12.130.140.150/17
25.	44.57.162.31	44.57.162.31/18
26.	152.154.66.65	152.154.66.65/20
27.	152.15.66.17	152.15.66.17/22
28.	132.45.171.88	132.45.171.88/21

Заключение: Выполнив эту практическую работу, Вы узнаете, каков формат IP-адреса, что такое маска сети, научитесь выделять составные части IP-адреса и определять по нему класс сети.

Протокол IP

Основу транспортных средств стека протоколов TCP/IP составляет протокол межсетевого взаимодействия *(Internet Protocol, IP).* Он обеспечивает передачу дейтаграмм от отправителя к получателям через объединенную систему компьютерных сетей.

Название данного протокола - *Internet Protocol* - отражает его суть: он должен передавать пакеты между сетями. В каждой очередной сети, лежащей на пути перемещения пакета, протокол IP вызывает средства транспортировки, принятые в этой сети, чтобы с их помощью передать этот пакет на маршрутизатор, ведущий к следующей сети, или непосредственно на узел-получатель.

Протокол IP относится к протоколам без установления соединений. Перед IP не ставится задача надежной доставки сообщений от отправителя к получателю. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных: отсутствует квитирование - обмен подтверждениями между отправителем и получателем, нет процедуры упорядочивания, повторных передач или других подобных функций. Если во время продвижения пакета произошла какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен по причине истечения времени жизни или из-за ошибки в контрольной сумме, то модуль IP не пытается заново послать испорченный или потерянный пакет. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP. Именно TCP организует повторную передачу пакетов, когда в этом возникает необходимость.

Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями. Свойство фрагментации во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

Имеется прямая связь между функциональной сложностью протокола и сложностью заголовка пакетов, которые этот протокол использует. Это объясняется тем, что основные служебные данные, на основании которых протокол выполняет то или иное действие, переносятся между двумя модулями, реализующими этот протокол на разных машинах,

именно в полях заголовков пакетов. Поэтому очень полезно изучить назначение каждого поля заголовка IP-пакета, и это изучение дает не только формальные знания о структуре пакета, но и объясняет все основные режимы работы протокола по обработке и передаче IP-дейтаграмм.

IP-адресация

Компьютер в сети может иметь адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и доменный адрес (DNS-имя).

- Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC - адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети.

- IP-адрес, используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла, например, 109.26.17.100.

Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса сети. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

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

Символьные доменные имена. Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях

разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу:RU - Россия, UK - Великобритания, SU - США), Примеров доменного имени может служить имя base2.sales.zil.ru. Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная распределенная служба Domain Name System (DNS), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также DNS-именами,

Классы IP-адресов. Для организации всемирной сети нужна хорошая система адресации, которая будет использоваться для направления информации всем адресатам. Союз Internet установил для адресации всех узлов Internet единый стандарт, называемый адресацией IP. Любой IP-адрес состоит из четырех чисел в интервале от 1 до 254, разделенных точками. Ниже приведен пример IP-адреса: 10.18.49.102. В схемах IP-адресации также могут использоваться числа 0 и 255, но они зарезервированы для специальных целей. Число 255 используется для направления дейтаграммы всем компьютерам сети IP. Число 0 используется для более точного указания адреса. Предположим, что в приведенном выше примере адрес служит для обозначения узла 102 в сети 10.18.49.102. В таком случае адрес 10.18.49.0 будет обозначать только сеть, а 0.0.0.102 будет обозначать один узел.

IP-адрес можно использовать для построения как сетей с несколькими узлами, так и сетей, содержащих миллионы узлов. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая - к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признаками того, к какому *классу* относится тот или иной IP-адрес.

На рисунке 1 показана структура IP-адреса разных классов.

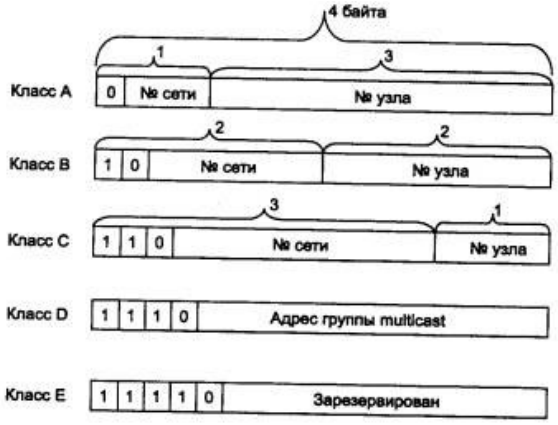


Рисунок 1 - Структура IP-адреса

Если адрес начинается с 0, то сеть относят к *классу A* и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей). Сетей класса A немного, зато количество узлов в них может достигать 2^{24}, то есть 16 777 216 узлов.

Если первые два бита адреса равны 10, то сеть относится к *классу B*. В сетях класса Впод номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса B является сетью средних размеров с максимальным числом узлов 2^{16}, что составляет 65 536 узлов.

Если адрес начинается с последовательности 110, то это сеть *класса C*. В этом случае под номер сети отводится 24 бита, а под номер узла - 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 28, то есть 256 узлами.

Если адрес начинается с последовательности 1110, то он является адресом *класса D и* обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к *классу E,* Адреса этого класса зарезервированы для будущих применений.

В таблице 1 приведены диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей.

Таблица 1- Характеристики адресов разного класса

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}

B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Большие сети получают адреса класса A, средние - класса B, а маленькие класса C.

Особые IP-адреса. В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов.

- Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет; этот режим используется только в некоторых сообщениях ICMP.

- Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.

- Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным.сообщением (limited broadcast)*.

- Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0. Такая рассылка называется *широковещательным сообщением (broadcast)*.

При адресации необходимо учитывать те ограничения, которые вносятся особым назначением некоторых IP-адресов. Так, ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей. Отсюда следует, что максимальное количество узлов, приведенное в таблице для сетей каждого класса, на практике должно быть уменьшено на 2. Например, в сетях класса C под номер узла отводится 8 бит, которые позволяют задавать 256 номеров: от 0 до 255. Однако на практике максимальное число узлов в сети класса C не может превышать 254, так как адреса 0 и 255 имеют специальное назначение. Из этих же соображений следует, что конечный узел не может иметь адрес типа 98.255.255.255, поскольку номер узла в этом адресе класса A состоит из одних двоичных единиц.

Особый смысл имеет IP-адрес, первый октет которого равен 127. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля». Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127. Этот

адрес имеет название *loopback*. Можно отнести адрес 127.0.0.0 ко внутренней сети модуля маршрутизации узла, а адрес 127.0.0.1 - к адресу этого модуля на внутренней сети. На самом деле любой адрес сети 127.0.0.0 служит для обозначения своего модуля маршрутизации, а не только 127.0.0.1, например 127.0.0.3.

В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть доставлены абсолютно всем узлам. Как ограниченный широковещательный IP-адрес, так и широковещательный IP-адрес имеют пределы распространения в интерсети - они ограничены либо сетью, к которой принадлежит узел-источник пакета, либо сетью, номер которой указан в адресе назначения. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей просто потому, что нет способа адресовать пакет одновременно всем узлам всех сетей составной сети.

Уже упоминавшаяся форма группового IP-адреса - *multicast* - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Члены какой-либо группы multicast не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по совершенно различным сетям, находящимся друг от друга на произвольном количестве хопов. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Основное назначение multicast-адресов - распространение информации по схеме «один-ко-многим». Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Management Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы.

Чтобы маршрутизаторы могли автоматически распространять пакеты с адресом multicast по составной сети, необходимо использовать в конечных маршрутизаторах модифицированные протоколы обмена маршрутной информацией, такие как, например, MOSPF (Multicast OSPF, аналог OSPF).

Групповая адресация предназначена для экономичного распространения в Internet или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой

аудитории слушателей или зрителей. Если такие средства найдут широкое применение (сейчас они представляют в основном небольшие экспериментальные островки в общем Internet), то Internet сможет создать серьезную конкуренцию радио и телевидению.

Использование масок в IP-адресации. Традиционная схема деления IP-адреса на номер сети и номер узла основана на понятии класса, который определяется значениями нескольких первых бит адреса. Именно потому, что первый байт адреса 185.23.44.206 попадает в диапазон 128-191, мы можем сказать, что этот адрес относится к классу B, а значит, номером сети являются первые два байта, дополненные двумя нулевыми байтами - 185.23.0.0, а номером узла - 0.0.44.206.

А что если использовать какой-либо другой признак, с помощью которого можно было бы более гибко устанавливать границу между номером сети и номером узла? В качестве такого признака сейчас получили широкое распространение маски. *Маска* - это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность.

Для стандартных классов сетей маски имеют следующие значения:

- класс A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- класс B - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
- класс C-11111111.11111111.11111111.00000000 (255.255.255.0).

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации. Например, если рассмотренный выше адрес 185.23.44.206 ассоциировать с маской 255.255.0.0, то номером сети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов.

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде:

IP-адрес 129.64.134.5 - 10000001. 01000000.10000110. 00000101

Маска 255.255.128.0 - 11111111.11111111.10000000. 00000000

Если игнорировать маску, то в соответствии с системой классов адрес 129.64.134.5 относится к классу B, а значит, номером сети являются первые 2 байта - 129.64.0.0, а номером узла - 0.0.134.5.

Если же использовать для определения границы номера сети маску, то 17 последовательных единиц в маске, «наложенные» на IP-адрес, определяют в качестве номера сети в двоичном выражении число:

10000001. 01000000. 10000000. 00000000 или в десятичной форме записи - номер сети 129.64.128.0, а номер узла 0.0.6.5.

Механизм масок широко распространен в IP-маршрутизации, причем маски могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей. На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых «префиксов» с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов.

Отображение IP-адресов на локальные адреса. Протокол ARP

Для отображения IP-адресов в Ethernet адреса используется протокол ARP (Address Resolution Protocol - адресный протокол). Отображение выполняется только для отправляемых IP-пакетов, так как только в момент отправки создаются заголовки IP и Ethernet.

ARP-таблица для преобразования адресов.Преобразование адресов выполняется путем поиска в таблице. Эта таблица, называемая ARP-таблицей, хранится в памяти и содержит строки для каждого узла сети. В двух столбцах содержатся IP- и Ethernet-адреса. Если требуется преобразовать IP-адрес в Ethernet-адрес, то ищется запись с соответствующим IP-адресом. Ниже приведен пример упрощенной ARP-таблицы.

Принято все байты 4-байтного IP-адреса записывать десятичными числами, разделенными точками. При записи 6-байтного Ethernet-адреса каждый байт указывается в 16-ричной системе и отделяется двоеточием.

Таблица 2 - Пример ARP-таблицы

IP-адрес	Ethernet-адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

ARP-таблица необходима потому, что IP-адреса и Ethernet-адреса выбираются независимо, и нет какого-либо алгоритма для преобразования одного в другой. IP-адрес выбирает менеджер сети с учетом положения машины в сети internet. Если машину перемещают в другую часть сети internet, то ее IP-адрес должен быть изменен. Ethernet-адрес выбирает производитель сетевого интерфейсного оборудования из выделенного для него по лицензии адресного пространства. Когда у машины заменяется плата сетевого адаптера, то меняется и ее Ethernet-адрес.

Порядок преобразования адресов. В ходе обычной работы сетевая программа, такая как TELNET, отправляет прикладное сообщение, пользуясь транспортными услугами TCP. Модуль TCP посылает соответствующее транспортное сообщение через модуль IP. В результате составляется IP-пакет, который должен быть передан драйверу Ethernet. IP-адрес места назначения известен прикладной программе, модулю TCP и модулю IP. Необходимо на его основе найти Ethernet-адрес места назначения. Для определения искомого Ethernet-адреса используется ARP-таблица.

Запросы и ответы протокола ARP. Как же заполняется ARP-таблица? Она заполняется автоматически модулем ARP, по мере необходимости. Когда с помощью существующей ARP-таблицы не удается преобразовать IP-адрес, то происходит следующее:

1) По сети передается широковещательный ARP-запрос.
2) Исходящий IP-пакет ставится в очередь.

Каждый сетевой адаптер принимает широковещательные передачи. Все драйверы Ethernet проверяют поле типа в принятом Ethernet-кадре и передают ARP-пакеты модулю ARP. ARP-запрос можно интерпретировать так: "Если ваш IP-адрес совпадает с указанным, то сообщите мне ваш Ethernet-адрес". Пакет ARP-запроса выглядит примерно так.

Таблица 3 - Пример ARP-запроса

IP-адрес отправителя	223.1.2.1
Ethernet-адрес отправителя	08:00:39:00:2F:C3
Искомый IP-адрес	223.1.2.2
Искомый Ethernet-адрес	<пусто>

Каждый модуль ARP проверяет поле искомого IP-адреса в полученном ARP-пакете и, если адрес совпадает с его собственным IP-адресом, то посылает ответ прямо по Ethernet-адресу отправителя запроса. ARP-ответ можно интерпретировать так: "Да, это мой IP-адрес, ему соответствует такой-то Ethernet-адрес". Пакет с ARP-ответом выглядит примерно так.

Таблица 4 - Пример ARP-ответа

IP-адрес отправителя	223.1.2.2
Ethernet-адрес отправителя	08:00:28:00:38:A9
Искомый IP-адрес	223.1.2.1
Искомый Ethernet-адрес	08:00:39:00:2F:C3

Этот ответ получает машина, сделавшая ARP-запрос. Драйвер этой машины проверяет поле типа в Ethernet-кадре и передает ARP-пакет модулю ARP. Модуль ARP анализирует

ARP-пакет и добавляет запись в свою ARP-таблицу. Обновленная таблица выглядит следующим образом.

Таблица 5 - ARP-таблица после обработки ответа

IP-адрес	Ethernet-адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.2	08:00:28:00:38:A9
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

Продолжение преобразования адресов.Новая запись в ARP-таблице появляется автоматически, спустя несколько миллисекунд после того, как она потребовалась. Как вы помните, ранее на шаге 2 исходящий IP-пакет был поставлен в очередь. Теперь с использованием обновленной ARP-таблицы выполняется преобразование IPадреса в Ethernet-адрес, после чего Ethernet-кадр передается по сети. Полностью порядок преобразования адресов выглядит так:

1) По сети передается широковещательный ARP-запрос.

2) Исходящий IP-пакет ставится в очередь.

3) Возвращается ARP-ответ, содержащий информацию о соответствии IP- и Ethernet-адресов. Эта информация заносится в ARP-таблицу.

4) Для преобразования IP-адреса в Ethernet-адрес у IP-пакета, поставленного в очередь, используется ARP-таблица.

5) Ethernet-кадр передается по сети Ethernet.

Короче говоря, если с помощью ARP-таблицы не удается сразу осуществить преобразование адресов, то IP-пакет ставится в очередь, а необходимая для преобразования информация получается с помощью запросов и ответов протокола ARP, после чего IP-пакет передается по назначению.

Если в сети нет машины с искомым IP-адресом, то ARP-ответа не будет и не будет записи в ARP-таблице. Протокол IP будет уничтожать IP-пакеты, направляемые по этому адресу. Протоколы верхнего уровня не могут отличить случай повреждения сети Ethernet от случая отсутствия машины с искомым IP-адресом.

Некоторые реализации IP и ARP не ставят в очередь IP-пакеты на то время, пока они ждут ARP-ответов. Вместо этого IP-пакет просто уничтожается, а его восстановление возлагается на модуль TCP или прикладной процесс, работающий через UDP. Такое восстановление выполняется с помощью таймаутов и повторных передач. Повторная

передача сообщения проходит успешно, так как первая попытка уже вызвала заполнение ARP-таблицы.

Следует отметить, что каждая машина имеет отдельную ARP-таблицу для каждого своего сетевого интерфейса.

IP-маршрутизация

Модуль IP является базовым элементом технологии Internet, а центральной частью IP является его таблица маршрутов. Протокол IP использует эту таблицу при принятии всех решений о маршрутизации IP-пакетов. Содержание таблицы маршрутов определяется администратором сети. Ошибки при установке маршрутов могут заблокировать передачи.

Чтобы понять технику межсетевого взаимодействия, нужно понять то, как используется таблица маршрутов. Это понимание необходимо для успешного администрирования и сопровождения IP-сетей.

Прямая маршрутизация.На рисунке показана небольшая IP-сеть, состоящая из 3 машин: A, B и C. Каждый сетевой адаптер этих машин имеет свой Ethernet-адрес. Менеджер сети должен присвоить машинам уникальные IP-адреса.

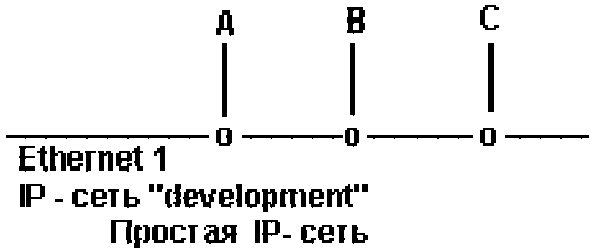


Рисунок 2 - Простая IP-сеть

Когда A посылает IP-пакет B, то заголовок IP-пакета содержит в поле отправителя IP-адрес узла A, а заголовок Ethernet-кадра содержит в поле отправителя Ethernet-адрес A. Кроме этого, IP-заголовок содержит в поле получателя IP-адрес узла B, а Ethernet-заголовок содержит в поле получателя Ethernet-адрес B.

Таблица 6 - Адреса в Ethernet-кадре, передающем IP-пакет от A к B

Адрес	Отправитель	Получатель
IP-заголовок	A	B
Ethernet-заголовок	A	B

В этом простом примере протокол IP является излишеством, которое мало что добавляет к услугам, предоставляемым сетью Ethernet. Однако протокол IP требует

дополнительных расходов на создание, передачу и обработку IP-заголовка. Когда в машине B модуль IP получает IP-пакет от машины A, он сопоставляет IP-адрес места назначения со своим, и если адреса совпадают, то передает дейтаграмму протоколу верхнего уровня.

В данном случае при взаимодействии A с B используется прямая маршрутизация.

Косвенная маршрутизация.На рисунке представлена более реалистичная картина сети Internet. В данном случае сеть Internet состоит из трех сетей Ethernet, на базе которых работают три IP-сети, объединенные шлюзом D. Каждая IP-сеть включает четыре машины; каждая машина имеет свои собственные IP- и Ethernet адреса.

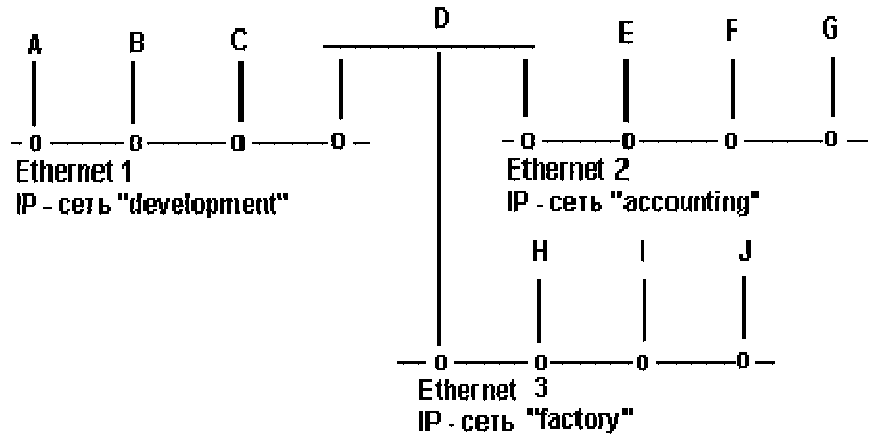


Рисунок 3 - Сеть Internet, состоящая из трех IP-сетей

Шлюз D соединяет все три сети и, следовательно, имеет три IP-адреса и три Ethernet-адреса. Машина D имеет три модуля ARP и три драйвера Ethernet. Обратим внимание на то, что машина D имеет только один модуль IP.

Менеджер сети присваивает каждой сети Ethernet уникальный номер, называемый IP-номером сети. На рисунке 15 IP-номера не показаны, вместо них используются имена сетей.

Когда машина A посылает IP-пакет машине B, то процесс передачи идет в пределах одной сети. При всех взаимодействиях между машинами, подключенными к одной IP-сети, используется прямая маршрутизация, обсуждавшаяся в предыдущем примере.

Когда машина D взаимодействует с машиной A, то это прямое взаимодействие. Когда машина D взаимодействует с машиной E, то это прямое взаимодействие. Когда машина D взаимодействует с машиной H, то это прямое взаимодействие. Это так, поскольку каждая пара этих машин принадлежит одной IP-сети.

Однако когда машина A взаимодействует с машинами, включенными в другую IP-сеть, то взаимодействие уже не будет прямым. Машина A должна использовать шлюз D для ретрансляции IP-пакетов в другую IP-сеть. Такое взаимодействие называется "косвенным".

Маршрутизация IP-пакетов выполняется модулями IP и является прозрачной для модулей TCP, UDP и прикладных процессов.

Если машина A посылает машине E IP-пакет, то IP-адрес и Ethernet-адрес отправителя соответствуют адресам A. IP-адрес места назначения является адресом E, но поскольку модуль IP в A посылает IP-пакет через D, Ethernet-адрес места назначения является адресом D.

Таблица 7 - Адреса в Ethernet-кадре, содержащем IP-пакет от A к E (до шлюза D).

Адрес	Отправитель	Получатель
IP-заголовок	A	E
Ethernet-заголовок	A	D

Модуль IP в машине D получает IP-пакет и проверяет IP-адрес места назначения. Определив, что это не его IP-адрес, шлюз D посылает этот IP-пакет прямо к E.

Таблица 8 - Адреса в Ethernet-кадре, содержащем IP-пакет от A к E (после шлюз D)

Адрес	Отправитель	Получатель
IP-заголовок	A	E
Ethernet-заголовок	D	E

Итак, при прямой маршрутизации IP- и Ethernet-адреса отправителя соответствуют адресам того узла, который послал IP-пакет, а IP- и Ethernet-адреса места назначения соответствуют адресам получателя. При косвенной маршрутизации IP- и Ethernet-адреса не образуют таких пар.

В данном примере сеть internet является очень простой. Реальные сети могут быть гораздо сложнее, так как могут содержать несколько шлюзов и несколько типов физических сред передачи. В приведенном примере несколько сетей Ethernet объединяются шлюзом для того, чтобы локализовать широковещательный трафик в каждой сети.

Правила маршрутизации в модуле IP.Рассмотрим правила или алгоритм маршрутизации. Для отправляемых IP-пакетов, поступающих от модулей верхнего уровня, модуль IP должен определить способ доставки - прямой или косвенный - и выбрать сетевой интерфейс. Этот выбор делается на основании результатов поиска в таблице маршрутов.

Для принимаемых IP-пакетов, поступающих от сетевых драйверов, модуль IP должен решить, нужно ли ретранслировать IP-пакет по другой сети или передать его на верхний уровень. Если модуль IP решит, что IP-пакет должен быть ретранслирован, то дальнейшая работа с ним осуществляется также, как с отправляемыми IP-пакетами.

Входящий IP-пакет никогда не ретранслируется через тот же сетевой интерфейс, через который он был принят.

Решение о маршрутизации принимается до того, как IP-пакет передается сетевому драйверу, и до того, как происходит обращение к ARP-таблице.

IP-таблица маршрутов. Как модуль IP узнает, какой именно сетевой интерфейс нужно использовать для отправления IP-пакета? Модуль IP осуществляет поиск в таблице маршрутов. Ключом поиска служит номер IP-сети, выделенный из IP-адреса места назначения IP-пакета.

Таблица маршрутов содержит по одной строке для каждого маршрута. Основными столбцами таблицы маршрутов являются номер сети, флаг прямой или косвенной маршрутизации, IP-адрес шлюза и номер сетевого интерфейса. Эта таблица используется модулем IP при обработке каждого отправляемого IP-пакета.

В большинстве систем таблица маршрутов может быть изменена с помощью команды "route". Содержание таблицы маршрутов определяется менеджером сети, поскольку менеджер сети присваивает машинам IP-адреса.

Подробности прямой маршрутизации. Рассмотрим более подробно, как происходит маршрутизация в одной физической сети.

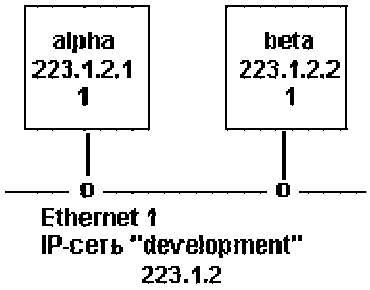


Рисунок 4 - Одна физическая сеть

Таблица маршрутов в узле alpha выглядит так.

Таблица 9 - Пример таблицы маршрутов

Сеть	Флаг вида маршрутизации	Шлюз	Номер интерфейса
development	Прямая	<пусто>	1

В данном простом примере все узлы сети имеют одинаковые таблицы маршрутов. Для сравнения ниже представлена та же таблица, но вместо названия сети указан ее номер.

Таблица 10 - Пример таблицы маршрутов с номерами сетей

Сеть	Флаг вида маршрутизации	Шлюз	Номер интерфейса
223.1.2	Прямая	<пусто>	1

Порядок прямой маршрутизации. Узел alpha посылает IP-пакет узлу beta. Этот пакет находится в модуле IP узла alpha, и IP-адрес места назначения равен IP-адресу beta (223.1.2.2). Модуль IP с помощью маски подсети выделяет номер сети из IP-адреса и ищет соответствующую ему строку в таблице маршрутов. В данном случае подходит первая строка.

Остальная информация в найденной строке указывает на то, что машины этой сети доступны напрямую через интерфейс номер 1. С помощью ARP-таблицы выполняется преобразование IP-адреса в соответствующий Ethernet-адрес, и через интерфейс 1 Ethernet-кадр посылается узлу beta.

Если прикладная программа пытается послать данные по IP-адресу, который не принадлежит сети development, то модуль IP не сможет найти соответствующую запись в таблице маршрутов. В этом случае модуль IP отбрасывает IP-пакет. Некоторые реализации протокола возвращают сообщение об ошибке "Сеть не доступна".

Подробности косвенной маршрутизации.Теперь рассмотрим более сложный порядок маршрутизации в IP-сети, изображенной на рисунке 17.

Таблица маршрутов в узле alpha выглядит так.

Таблица 11 - Таблица маршрутов в узле alpha

Сеть	Флаг вида маршрутизации	Шлюз	Номер интерфейса
development	прямая	<пусто>	1
accounting	косвенная	devnetrouter	1
factory	косвенная	devnetrouter	1

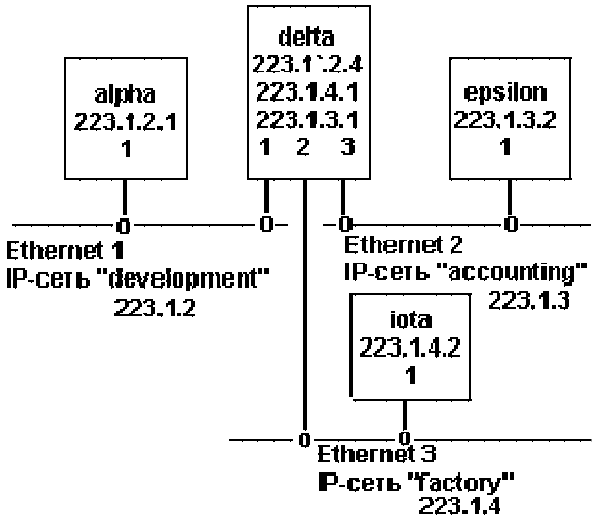


Рисунок 5 - Подробная схема трех сетей

Та же таблица с IP-адресами вместо названий.

Таблица 12 - Таблица маршрутов в узле alpha (с номерами)

Сеть	Флаг вида маршрутизации	Шлюз	Номер интерфейса
223.1.2	прямая	<пусто>	1
223.1.3	косвенная	223.1.2.4	1
223.1.4	косвенная	223.1.2.4	1

В столбце "шлюз" таблицы маршрутов узла alpha указывается IP-адрес точки соединения узла delta с сетью development.

Порядок косвенной маршрутизации.Узел alpha посылает IP-пакет узлу epsilon. Этот пакет находится в модуле IP узла alpha, и IP-адрес места назначения равен IP-адресу узла epsilon (223.1.3.2). Модуль IP выделяет сетевой номер из IP-адреса (223.1.3) и ищет соответствующую ему строку в таблице маршрутов. Соответствие находится во второй строке.

Запись в этой строке указывает на то, что машины требуемой сети доступны через шлюз devnetrouter. Модуль IP в узле alpha осуществляет поиск в ARP-таблице, с помощью которого определяет Ethernet-адрес, соответствующий IP-адресу devnetrouter. Затем IP-пакет, содержащий IP-адрес места назначения epsilon, посылается через интерфейс 1 шлюзу devnetrouter.

IP-пакет принимается сетевым интерфейсом в узле delta и передается модулю IP. Проверяется IP-адрес места назначения, и, поскольку он не соответствует ни одному из собственных IP-адресов delta, шлюз решает ретранслировать IP-пакет. Модуль IP в узле delta выделяет сетевой номер из IP-адреса места назначения IP-пакета (223.1.3) и ищет соответствующую запись в таблице маршрутов. Таблица маршрутов в узле delta выглядит так.

Таблица 13 - Таблица маршрутов в узле delta

Сеть	Флаг вида маршрутизации	Шлюз	Номер интерфейса
development	прямая	<пусто>	1
accounting	прямая	<пусто>	2
factory	прямая	<пусто>	3

Та же таблица с IP-адресами вместо названий.

Таблица 14 - Таблица маршрутов в узле delta (с номерами)

Сеть	Флаг вида маршрутизации	Шлюз	Номер интерфейса
223.1.2	прямая	<пусто>	1
223.1.3	прямая	<пусто>	2
223.1.4	прямая	<пусто>	3

Соответствие находится во второй строке. Теперь модуль IP напрямую посылает IP-пакет узлу epsilon через интерфейс номер 2. Пакет содержит IP- и Ethernet-адреса места назначения равные epsilon.

Узел epsilon принимает IP-пакет, и его модуль IP проверяет IP-адрес места назначения. Он соответствует IP-адресу epsilon, поэтому содержащееся в IP-пакете сообщение передается протокольному модулю верхнего уровня.

Формат заголовка IP-дейтаграммы

IP-дейтаграмма состоит из заголовка и данных. Заголовок дейтаграммы состоит из 32-разрядных слов и имеет переменную длину, зависящую от размера поля “Options”, но всегда кратную 32 битам. За заголовком непосредственно следуют данные, передаваемые в дейтаграмме (рисунок 6).

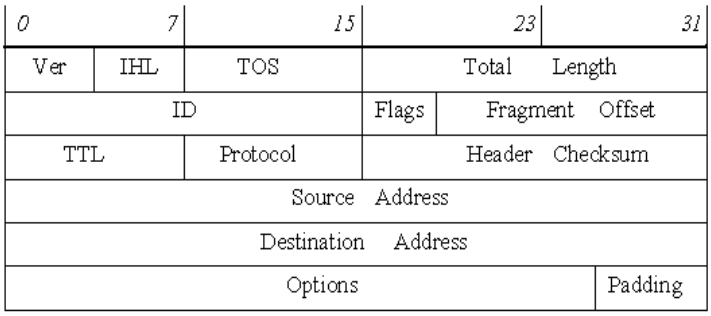


Рисунок 6 - Формат заголовка IP-дейтаграммы

Значения полей заголовка следующие.

Ver (4 бита) - версия протокола IP, в настоящий момент используется версия 4, новые разработки имеют номера версий 6-8.

IHL (Internet Header Length) (4 бита) - длина заголовка в 32-битных словах; диапазон допустимых значений от 5 (минимальная длина заголовка, поле “Options” отсутствует) до 15 (т.е. может быть максимум 40 байт опций).

TOS (Type Of Service) (8 бит) - значение поля определяет приоритет дейтаграммы и желаемый тип маршрутизации. Структура байта TOS представлена на рисунке 7.

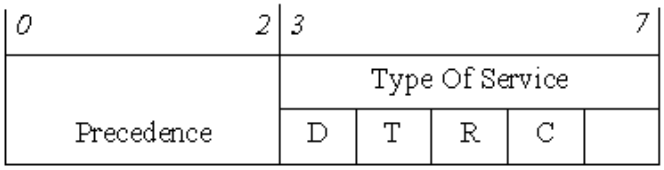


Рисунок 7 - Структура байта TOS

Три младших бита (“Precedence”) определяют приоритет дейтаграммы: 111 - управление сетью, 110 - межсетевое управление, 101 - CRITIC-ECP, 100 - более чем мгновенно, 011 – мгновенно, 010 – немедленно, 001 – срочно, 000 – обычно.

Биты D,T,R,C определяют желаемый тип маршрутизации:

- D (Delay) - выбор маршрута с минимальной задержкой,
- T (Throughput) - выбор маршрута с максимальной пропускной способностью,
- R (Reliability) - выбор маршрута с максимальной надежностью,
- C (Cost) - выбор маршрута с минимальной стоимостью.

В дейтаграмме может быть установлен только один из битов D,T,R,C. Старший бит байта не используется.

Реальный учет приоритетов и выбора маршрута в соответствии со значением байта TOS зависит от маршрутизатора, его программного обеспечения и настроек. Маршрутизатор может поддерживать расчет маршрутов для всех типов TOS, для части или игнорировать

TOS вообще. Маршрутизатор может учитывать значение приоритета при обработке всех дейтаграмм или при обработке дейтаграмм, исходящих только из некоторого ограниченного множества узлов сети, или вовсе игнорировать приоритет.

Total Length (16 бит) - длина всей дейтаграммы в октетах, включая заголовок и данные, максимальное значение 65535, минимальное - 21 (заголовок без опций и один октет в поле данных).

ID (Identification) (16 бит), **Flags** (3 бита), **Fragment Offset** (13 бит) используются для фрагментации и сборки дейтаграмм.

TTL (Time To Live) (8 бит) - "время жизни" дейтаграммы. Устанавливается отправителем, измеряется в секундах. Каждый маршрутизатор, через который проходит дейтаграмма, переписывает значение TTL, предварительно вычтя из него время, потраченное на обработку дейтаграммы. Так как в настоящее время скорость обработки данных на маршрутизаторах велика, на одну дейтаграмму тратится обычно меньше секунды, поэтому фактически каждый маршрутизатор вычитает из TTL единицу. При достижении значения TTL=0 дейтаграмма уничтожается, при этом отправителю может быть послано соответствующее ICMP-сообщение. Контроль TTL предотвращает зацикливание дейтаграммы в сети.

Protocol (8 бит) - определяет программу (вышестоящий протокол стека), которой должны быть переданы данные дейтаграммы для дальнейшей обработки.

Header Checksum (16 бит) - контрольная сумма заголовка, представляет из себя 16 бит, дополняющие биты в сумме всех 16-битовых слов заголовка. Перед вычислением контрольной суммы значение поля "Header Checksum" обнуляется. Поскольку маршрутизаторы изменяют значения некоторых полей заголовка при обработке дейтаграммы (как минимум, поля "TTL"), контрольная сумма каждым маршрутизатором пересчитывается заново. Если при проверке контрольной суммы обнаруживается ошибка, дейтаграмма уничтожается.

Source Address (32 бита) - IP-адрес отправителя.

Destination Address (32 бита) - IP-адресполучателя.

Options - опции, поле переменной длины. Опций может быть одна, несколько или ни одной. Опции определяют дополнительные услуги модуля IP по обработке дейтаграммы, в заголовок которой они включены.

Padding - выравнивание заголовка по границе 32-битного слова, если список опций занимает нецелое число 32-битных слов. Поле "Padding" заполняется нулями.

Протокол ICMP

Протокол ICMP(Internet Control Message Protocol, Протокол Управляющих Сообщений Интернет) выполняет следующие задачи:

- сообщает узлу-источнику об отказах маршрутизации;

- проверяет способности узлов образовывать повторное эхо в объединенной сети (сообщения Echo и ReplyICMP);

- стимулирует более эффективную маршрутизацию (с помощью сообщений RedirectICMP - переадресации ICMP);

- информирует узел-источник о том, что некоторая дейтаграмма превысила назначенное ей время существования в пределах данной сети (сообщение TimeExceededICMP - "время превышено");

- обеспечивает для новых узлов возможность нахождения маски подсети, используемой в объединенной сети в данный момент.

Протокол ICMP является неотъемлемой частью IP-модуля. Он обеспечивает обратную связь в виде диагностических сообщений, посылаемых отправителю при невозможности доставки его дейтаграммы и в других случаях.

ICMP-сообщения не порождаются при невозможности доставки:

– дейтаграмм, содержащих ICMP-сообщения;

– не первых фрагментов дейтаграмм;

– дейтаграмм, направленных по групповому адресу (широковещание, мультикастинг);

– дейтаграмм, адрес отправителя которых нулевой или групповой. Все ICMP-сообщения имеют IP-заголовок, значение поля “Protocol” равно 1.

Данные дейтаграммы с ICMP-сообщением не передаются вверх по стеку протоколов для обработки, а обрабатываются IP-модулем.

После IP-заголовка следует 32-битное слово с полями “Тип”, “Код” и “Контрольная сумма”. Поля типа и кода определяют содержание ICMP-сообщения. Формат остальной части дейтаграммы зависит от вида сообщения.

Контрольная сумма считается так же, как и в IP-заголовке, но в этом случае суммируется содержимое ICMP-сообщения, включая поля “Тип” и “Код”.

Протокол дейтаграмм пользователя UDP

Протокол UDP (User Datagram Protocol, протокол пользовательских дейтаграмм) используется в тех случаях, когда мощные средства обеспечения надежности протокола TCP не требуются. Протокол UDP обеспечивает ненадежную доставку дейтаграмм и не поддерживает соединений из конца в конец. К заголовку IP-пакета он добавляет два поля, одно из которых, поле "порт", обеспечивает мультиплексирование информации между разными прикладными процессами, а другое поле - "контрольная сумма" - позволяет поддерживать целостность данных. Реализация UDP намного проще, чем TCP.

Протокол UDP используется либо при пересылке коротких сообщений, когда накладные расходы на установление сеанса и проверку успешной доставки данных оказываются выше расходов на повторную (в случае неудачи) пересылку сообщения, либо в том случае, когда сама организация процесса-приложения обеспечивает установление соединения и проверку доставки пакетов (например, NFS).

Пользовательские данные, поступившие от прикладного уровня, предваряются UDP-заголовком, и сформированный таким образом UDP-пакет отправляется на межсетевой уровень. UDP-заголовок состоит из двух 32-битных слов (рисунок 8).

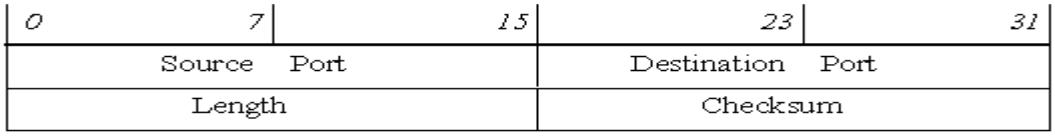


Рисунок 8 - UDP-заголовок

Заголовок UDP имеет четыре поля:

- порт источника (sourceport) - те же функции, что и в заголовке TCP;
- порт пункта назначения (destinationport) - те же функции, что и в заголовке TCP;
- длина (length) - длина заголовка UDP и данных;
- контрольная сумма (checksum) - обеспечивает проверку целостности пакета (факультативная возможность).

Контрольное суммирование.Контрольная сумма вычисляется таким же образом, как и в TCP-заголовке.Когда модуль UDP получает дейтаграмму от модуля IP, он проверяет контрольную сумму, содержащуюся в ее заголовке. Если контрольная сумма равна нулю, то это означает, что отправитель дейтаграммы ее не подсчитывал, и, следовательно, ее нужно игнорировать. Если два модуля UDP взаимодействуют только через одну сеть Ethernet, то от контрольного суммирования можно отказаться, так как средства Ethernet обеспечивают достаточную степень надежности обнаружения ошибок передачи. Это снижает накладные расходы, связанные с работой UDP. Однако рекомендуется всегда выполнять контрольное суммирование, так как возможно в какой-то момент изменения в таблице маршрутов приведут к тому, что дейтаграммы будут посылаться через менее надежную среду.

Если контрольная сумма правильная, то проверяется порт назначения, указанный в заголовке дейтаграммы. Если к этому порту подключен прикладной процесс, то прикладное сообщение, содержащееся в дейтаграмме, становится в очередь для прочтения. В остальных случаях дейтаграмма отбрасывается. Если дейтаграммы поступают быстрее, чем их успевает обрабатывать прикладной процесс, то при переполнении очереди сообщений поступающие дейтаграммы отбрасываются модулем UDP.

После заголовка непосредственно следуют пользовательские данные, переданные модулю UDP прикладным уровнем за один вызов. Протокол UDP рассматривает эти данные как целостное сообщение; он никогда не разбивает сообщение для передачи в нескольких пакетах и не объединяет несколько сообщений для пересылки в одном пакете. Если прикладной процесс N раз вызвал модуль UDP для отправки данных (т.е. запросил отправку N сообщений), то модулем UDP будет сформировано и отправлено N пакетов, и процесс-получатель будет должен N раз вызвать свой модуль UDP для получения всех сообщений.

При получении пакета от межсетевого уровня модуль UDP проверяет контрольную сумму и передает содержимое сообщения прикладному процессу, чей номер порта указан в поле “Destination Port”.

Максимальная длина UDP-сообщения равна максимальной длине IP-дейтаграммы (65535 октетов) за вычетом минимального IP-заголовка (20) и UDP-заголовка (8), т.е. 65507 октетов. На практике обычно используются сообщения длиной 8192 октета.

Примеры прикладных процессов, использующих протокол UDP: NFS (Network File System - сетевая файловая система), TFTP (Trivial File Transfer Protocol - простой протокол передачи файлов), SNMP (Simple Network Management Protocol - простой протокол управления сетью), DNS (Domain Name Service - доменная служба имен).

Порты. Взаимодействие между прикладными процессами и модулем UDP осуществляется через UDP-порты. Порты нумеруются, начиная с нуля. Прикладной процесс, предоставляющий некоторые услуги другим прикладным процессам (сервер), ожидает поступления сообщений в порт, специально выделенный для этих услуг. Сообщения должны содержать запросы на предоставление услуг. Они отправляются процессами-клиентами.

Например, сервер SNMP всегда ожидает поступлений сообщений в порт 161. Если клиент SNMP желает получить услугу, он посылает запрос в UDP порт 161 на машину, где работает сервер. В каждом узле может быть только один сервер SNMP, так как существует только один UDP-порт 161. Данный номер порта является общеизвестным, то есть фиксированным номером, официально выделенным для услуг SNMP. Общеизвестные номера определяются стандартами Internet.

По номеру порта транспортные протоколы определяют, какому приложению передать содержимое пакетов.

2.8 Лабораторная работа № 8, 9 (4 часа)

Тема: «Методы кодирования»

2.8.1 Цель работы: изучить способы кодирования информации в вычислительных сетях.

2.8.2 Задачи работы:

1. рассмотреть методы физического кодирования;
2. ознакомиться с методами повышения помехоустойчивости передачи и приема;
3. разработать программу для кодирования информации.

2.8.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.8.4 Описание (ход) работы:

1. Методы физического кодирования

При выборе способа кодирования нужно одновременно стремиться к достижению нескольких целей:

- минимизировать ширину спектра сигнала, полученного в результате кодирования;
- обеспечивать синхронизацию между передатчиком и приемником;
- обеспечивать устойчивость к шумам;
- обнаруживать и по возможности исправлять битовые ошибки;
- минимизировать мощность передатчика.

Более узкий спектр сигнала позволяет на одной и той же линии (с одной и той же полосой пропускания) добиваться более высокой скорости передачи данных. Спектр сигнала в общем случае зависит как от способа кодирования, так и от тактовой частоты передатчика.

Требования, предъявляемые к методам кодирования, являются взаимно противоречивыми, поэтому каждый из рассматриваемых далее популярных методов кодирования обладает своими достоинствами и недостатками в сравнении с другими.

Метод биполярного кодирования с альтернативной инверсией (AMI)

Одной из модификаций метода NRZ является метод биполярного кодирования с альтернативной инверсией (Bipolar Alternate Mark Inversion, AMI). В этом методе используются три уровня потенциала — отрицательный, нулевой и положительный. Для кодирования логического нуля используется нулевой потенциал, а логическая единица кодируется либо положительным потенциалом, либо отрицательным, при этом потенциал каждой новой единицы противоположен потенциалу предыдущей.

Код AMI частично ликвидирует проблемы постоянной составляющей и отсутствия самосинхронизации, присущие коду NRZ. Это происходит при передаче длинных последовательностей единиц. В этих случаях сигнал на линии представляет собой последовательность разнополярных импульсов с тем же спектром, что и у кода NRZ,

передающего чередующиеся нули и единицы, то есть без постоянной составляющей и с основной гармоникой N/2 Гц (где N — битовая скорость передачи данных). Длинные же последовательности нулей также опасны для кода AMI, как и для кода NRZ — сигнал вырождается в постоянный потенциал нулевой амплитуды. Поэтому код AMI требует дальнейшего улучшения.

Потенциальный код с инверсией при единице (NRZI)

Существует код, похожий на AMI, но только с двумя уровнями сигнала. При передаче нуля он передает потенциал, который был установлен в предыдущем такте (то есть не меняет его), а при передаче единицы потенциал инвертируется на противоположный. Этот код называется потенциальным кодом с инверсией при единице (Non Return to Zero with ones Inverted, NRZI). Этот код удобен в тех случаях, когда использование третьего уровня сигнала весьма нежелательно, например в оптических кабелях, где устойчиво распознаются два состояния сигнала - свет и темнота. Для улучшения потенциальных кодов, подобных AMI и NRZI, используются два метода. Первый метод основан на добавлении в исходный код избыточных бит, содержащих логические единицы. В этом случае длинные последовательности 0-ей прерываются, и код становится самосинхронизирующимся для любых передаваемых данных. Исчезает также постоянная составляющая, а значит, еще более сужается спектр сигнала. Но этот метод снижает полезную пропускную способность линии, так как избыточные единицы пользовательской информации не несут.

Манчестерский код

Манчестерский код (или код Манчестер-II) получил наибольшее распространение в локальных сетях. Он также относится к самосинхронизирующимся кодам, имеет два уровня, что способствует его лучшей помехозащищенности и упрощению приемных и передающих узлов. Логическому нулю соответствует положительный переход в центре битового интервала (то есть первая половина битового интервала – низкий уровень, вторая половина – высокий), а логической единице соответствует отрицательный переход в центре битового интервала (или наоборот).

Обязательное наличие перехода в центре бита позволяет приемнику манчестерского кода легко выделить из пришедшего сигнала синхросигнал и передать информацию сколь угодно большими последовательностями без потерь из-за рассинхронизации.

Потенциальный код 2B1Q

Код 2B1Q его название отражает суть — каждые два бита (2B) передаются за один такт (1) сигналом, имеющим четыре состояния (Q — Quadra). Паре битов 00 соответствует потенциал -2,5 В, паре 01 — потенциал -0,833 В, паре 11 — потенциал +0,833 В, а паре 10 — потенциал +2,5 В.

При этом способе кодирования требуются дополнительные меры по борьбе с длинными последовательностями одинаковых пар битов, так как при этом сигнал превращается в постоянную составляющую. При случайном чередовании битов спектр сигнала в два раза уже, чем у кода NRZ, так как при той же битовой скорости длительность такта увеличивается в два раза. Таким образом, с помощью кода 2B1Q можно по одной и той же линии передавать данные в два раза быстрее, чем с помощью кода AMI или NRZI.

Однако для его реализации мощность передатчика должна быть выше, чтобы четыре уровня четко различались приемником на фоне помех. Для улучшения потенциальных кодов типа AMI, NRZI или 2Q1B используются избыточные коды и скрэмблирование.

2. Методы повышения помехоустойчивости передачи и приема.

Логическое кодирование используется для улучшения потенциальных кодов типа AMI, NRZI, 2Q1B и уменьшения помех в сети. Логическое кодирование должно заменять длинные последовательности бит, приводящие к постоянному потенциалу (перегрев оборудования), вкраплениями единиц. Для логического кодирования характерны два метода - избыточные коды и скрэмблирование.

Избыточные коды

Избыточные коды основаны на разбиении исходной последовательности битов на порции, которые часто называют символами. Затем каждый исходный символ заменяется новым с большим количество битов, чем исходный.

Например, в логическом **коде 4B/5B**, используемом в технологиях FDDI и FastEthernet, исходные символы длиной 4 бит заменяются символами длиной 5 бит. Так как результирующие символы содержат избыточные биты, то общее количество битовых комбинаций в них больше, чем в исходных.

Таблица 1. Соответствие исходных и результирующих кодов 4B/5B

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

Скремблирование

Методы скремблирования заключаются в побитном вычислении результирующего кода на основании бит исходного кода и полученных в предыдущих тактах бит результирующего кода. Например, скремблер может реализовывать следующее соотношение:

$B_i = A_i \oplus B_{i-3} \oplus B_{i-5}$,

где B_i — двоичная цифра результирующего кода, полученная на i-м такте работы скремблера,A_i — двоичная цифра исходного кода, поступающая на i-м такте на

вход скремблера, B_{i-3} и B_{i-5} — двоичные цифры результирующего кода, полученные на предыдущих тактах работы скремблера, соответственно на 3 и на 5 тактов ранее текущего такта, ⊕— операция исключающего ИЛИ (сложение по модулю 2).

Например, для исходной последовательности 110110000001 скремблер даст следующий результирующий код:

$B_1 = A_1 = 1$ (первые три цифры результирующего кода будут совпадать с исходным, так как еще нет нужных предыдущих цифр)

$B_2 = A_2 = 1$

$B_3 = A_3 = 0$

$B_4 = A_4 \oplus B_1 = 1 \oplus 1 = 0$

$B_5 = A_5 \oplus B_2 = 1 \oplus 1 = 0$

$B_6 = A_6 \oplus B_3 \oplus B_1 = 0 \oplus 0 \oplus 1 = 1$

$B_7 = A_7 \oplus B_4 \oplus B_2 = 0 \oplus 0 \oplus 1 = 1$

$B_8 = A_8 \oplus B_5 \oplus B_3 = 0 \oplus 0 \oplus 0 = 0$

$B_9 = A_9 \oplus B_6 \oplus B_4 = 0 \oplus 1 \oplus 0 = 1$

$B_{10} = A_{10} \oplus B_7 \oplus B_5 = 0 \oplus 1 \oplus 0 = 1$

$B_{11} = A_{11} \oplus B_8 \oplus B_6 = 0 \oplus 0 \oplus 1 = 1$

$B_{12} = A_{12} \oplus B_9 \oplus B_7 = 1 \oplus 1 \oplus 1 = 1$

Таким образом, на выходе скремблера появится последовательность 110001101111, в которой нет последовательности из шести нулей, присутствовавшей в исходном коде.

После получения результирующей последовательности приемник передает ее дескремблеру, который восстанавливает исходную последовательность на основании обратного соотношения:

$C_i = B_i \oplus B_{i-3} \oplus B_{i-5} = (A_i \oplus B_{i-3} \oplus B_{i-5}) \oplus B_{i-3} \oplus B_{i-5} = A_i$.

Существуют и более простые методы борьбы с последовательностями единиц, также относимые к классу скрэмблирования.

Для улучшения кода AMI используются два метода, основанные на искусственном искажении последовательности нулей запрещенными символами.

На рисунке 2 показано использование метода B8ZS (Bipolarwith 8-Zeros Substitution) и метода HDB3 (High-DensityBipolar 3-Zeros) для корректировки кода AMI. Исходный код состоит из двух длинных последовательностей нулей: в первом случае - из 8, а во втором - из 5.

Рис. 2 Коды B8ZS и HDB3. V - сигнал единицы запрещенной полярности; 1*-сигнал единицы корректной полярности, но заменившей 0 в исходном коде.

Код B8ZS исправляет только последовательности, состоящие из 8 нулей. Для этого он после первых трех нулей вместо оставшихся пяти нулей вставляет пять цифр: V-1*-0-V-1*. V здесь обозначает сигнал единицы, запрещенной для данного такта полярности, то есть сигнал, не изменяющий полярность предыдущей единицы, 1* - сигнал единицы корректной полярности, а знак звездочки отмечает тот факт, что в исходном коде в этом такте была не единица, а ноль. В результате на 8 тактах приемник наблюдает 2 искажения - очень маловероятно, что это случилось из-за шума на линии или других сбоев передачи. Поэтому приемник считает такие нарушения кодировкой 8 последовательных нулей и после приема заменяет их на исходные 8 нулей. Код B8ZS построен так, что его постоянная составляющая равна нулю при любых последовательностях двоичных цифр.

Код HDB3 исправляет любые четыре подряд идущих нуля в исходной последовательности. Правила формирования кода: каждые четыре нуля заменяются четырьмя сигналами, в которых имеется один сигнал V. Для подавления постоянной составляющей полярность сигнала V чередуется при последовательных заменах. Для замены используются два образца четырехтактовых кодов. Если перед заменой исходный код содержал нечетное число 1-ц, то используется последовательность 000V, а если число 1-ц было четным - последовательность 1*00V.

Улучшенные потенциальные коды обладают достаточно узкой полосой пропускания для любых последовательностей единиц и нулей, которые встречаются в передаваемых данных.

3. Задание

Необходимо разработать программу для кодирования информации, используя код (по варианту), при этом для устранения последовательностей нулей использовать логическое кодирование (по варианту). Входную последовательность информации ввести с клавиатуры. Результаты работы отобразить в виде временной диаграммы, при этом на диаграмме должны быть:

- входная последовательность в коде NRZ,
- входная последовательность в виде самосинхронизирующегося кода (по варианту),
- входная последовательность в логическом коде (по варианту).

4. Варианты задания:

№ варианта	Самосинхронизирующиеся коды	Логическое кодирование
1	Биполярный код AMI	Избыточный код 4B/5B
2	Код NRZI	Скремблер со сдвигом 3 и 5
3	Манчестерский код	Избыточный код 4B/5B
4	Биполярный код AMI	Метод B8ZS
5	Код NRZI	Скремблер со сдвигами 3 и 5 позиции
6	Биполярный код AMI	Метод HDB3
7	Манчестерский код	Метод B8ZS
8	Код NRZI	Скремблер со сдвигом 5 и 8
9	Биполярный код AMI	Скремблер со сдвигом 3 и 5
10	Манчестерский код	Скремблер со сдвигом 3 и 5
11	Код NRZI	Метод B8ZS
12	Биполярный код AMI	Скремблер со сдвигами 5 и 13 позиции
13	Код NRZI	Метод HDB3
14	Код 2B1Q	Избыточный код 4B/5B
15	Код 2B1Q	Скремблер со сдвигом 3 и 5
16	Код 2B1Q	Метод B8ZS
17	Манчестерский код	Скремблер со сдвигами 5 и 13 позиции

5. Структура отчета

1. титульный лист;
2. цель работы, задание;
3. краткие теоретические сведения;
4. алгоритм работы программы;
5. листинг программы кодирования информации;
6. результаты работы программы;
7. выводы.

2.9 Лабораторная работа № 10, 11 (4 часа)

Тема: «Освоение графического интерфейса NetCracker»

2.9.1 Цель работы: освоение графического интерфейса NetCracker, знакомство с главными приложениями данной программы и общими принципами моделирования сети в ней.

2.9.2 Задачи работы:

1. ознакомиться с графическим интерфейсом NetCracker.

2.9.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.9.4 Описание (ход) работы:

NetCracker Professional – программный пакет, разработанный фирмой NetCracker Technology (http://www.netcracker.com), позволяет создавать проекты вычислительных сетей разной сложности и топологий, используя технологию имитационного моделирования работы сети.

Откройте файл с текстом лабораторной работы и запустите из стартового меню саму программу. Далее, читайте и выполняйте задания.

Главное окно приложения показано на рис.1. Оно состоит из браузера оборудования, рабочего окна и главного меню.

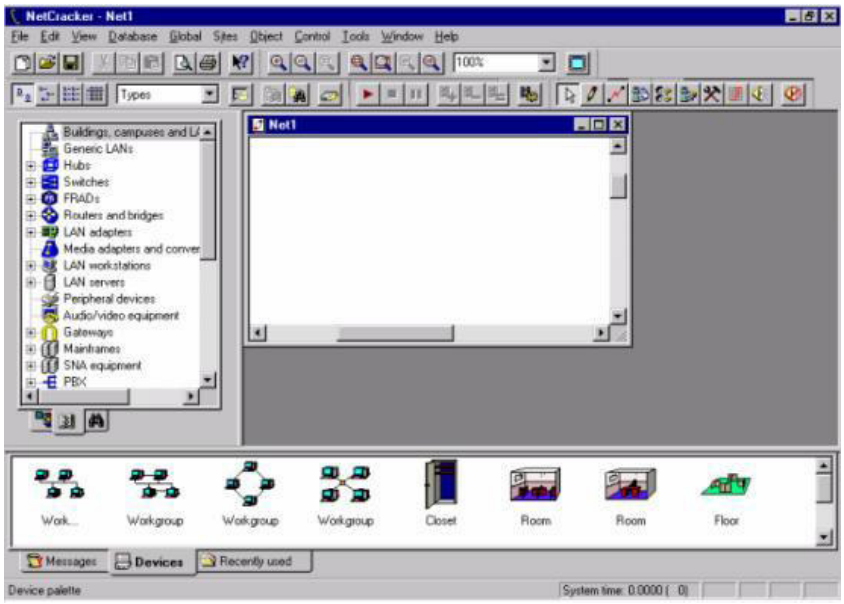


Рис.1.

Познакомьтесь с содержимым главного меню программы.

2. Откройте файл-пример проекта сетиNetCracker Professional (.NET) file File menu select Open

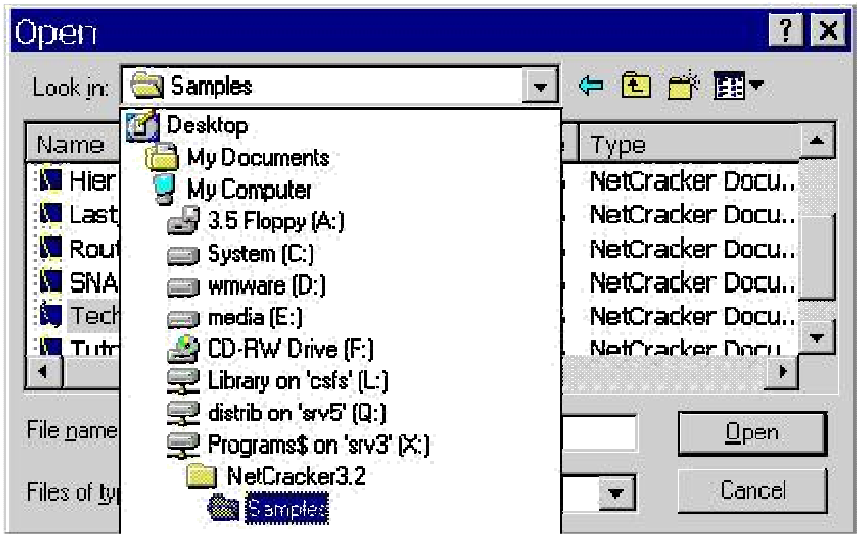


Рис.2.

Выберете файл Techno.net , нажав кнопку Open или двойным щелчком левой кнопки мыши. Проект сети загрузится в рабочее окно рис.3.

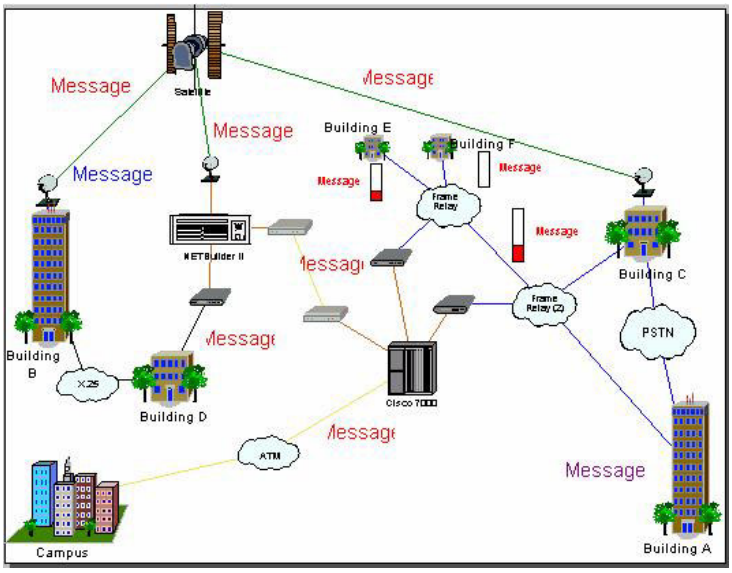
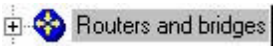


Рис.3.

Масштаб просмотра можно регулировать семейством кнопок Zoom 

С помощью линейки прокрутки ознакомьтесь с содержанием браузера оборудования (закладка Devices). Группы устройств, помеченные в узлах знаком “+”, раскрываются на составляющие.



Поиск оборудования, содержащегося в БД Net Cracker, можно производить разными способами:

Database □ Hierarchy □ Types (классификация по типам оборудования)

Database □ Hierarchy □ Vendors (классификация по фирмам изготови-лелям)

Например, Вам необходимо выбрать сервер Super Stack II Edge Server Pro 3000 001945-0. Для этого выберем 3 Com Corp.LAN Server

В результате Вы увидите в нижнем окне семейство LAN Server компании

3ComCorp. Выбрав необходимый из них (Super Stack II Edge Server Pro 3000 001945-0) левой кнопкой мыши, вы увидите полный набор его технических характеристик.

Используя Database toolbar, можно осуществлять просмотр и поиск обору-дования в разном виде: текстовом и графическом.

Заметим, что если Вы не желаете использовать в своем проекте конкретное оборудование конкретных производителей, то можете воспользоваться абстрактными устройствами из раздела Database Hierarchy Ven-dors Generic Devices .

Поиск оборудования производится также из раздела меню Database:Database

 Find Condition=Description includes например,

FrameRelay. Результаты поиска будут отображаться на закладке браузера оборудования «CompatibleDevices». Перейти к обычному режиму браузера можно выбравзакладку «Devices».

В открытом файле-проекте сети Вы можете посмотреть и изменить характеристики оборудования, включенного в проект. Например, у Вас открыт в данный момент файл Techno.net . Дважды щелкните мышкой по маршрутизатору Cisco 7000, в результате появиться окно конфигурации Cisco 7000(рис.4).

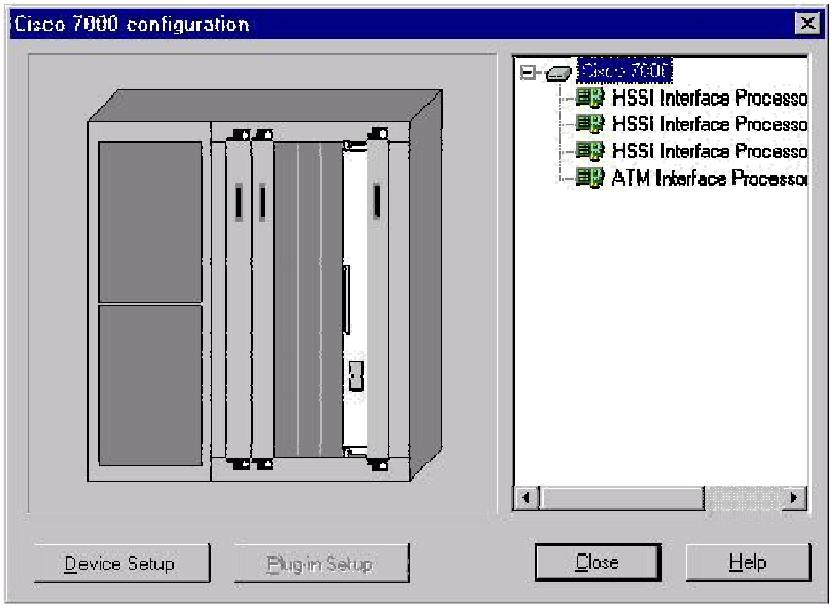


Рис.4.

При нажатии кнопки Device Setup появляется окно с описанием свойств Cisco 7000.

Если мы хотим получить информацию об устройствах, которыми укомплектован маршрутизатор Cisco 7000 из проекта Techno.net, нам нужно выбрать название устройства и нажать кнопку PluginSetup. Того же самого можно достичь выбрав название устройства и

нажав правую кнопку мыши, затем в меню выбрать Properties (здесь можно также и прослушать название устройства по-английски Say description).

Например, посмотрим свойстваATM Interface Processor TAXI multi-mode (Рис.5).

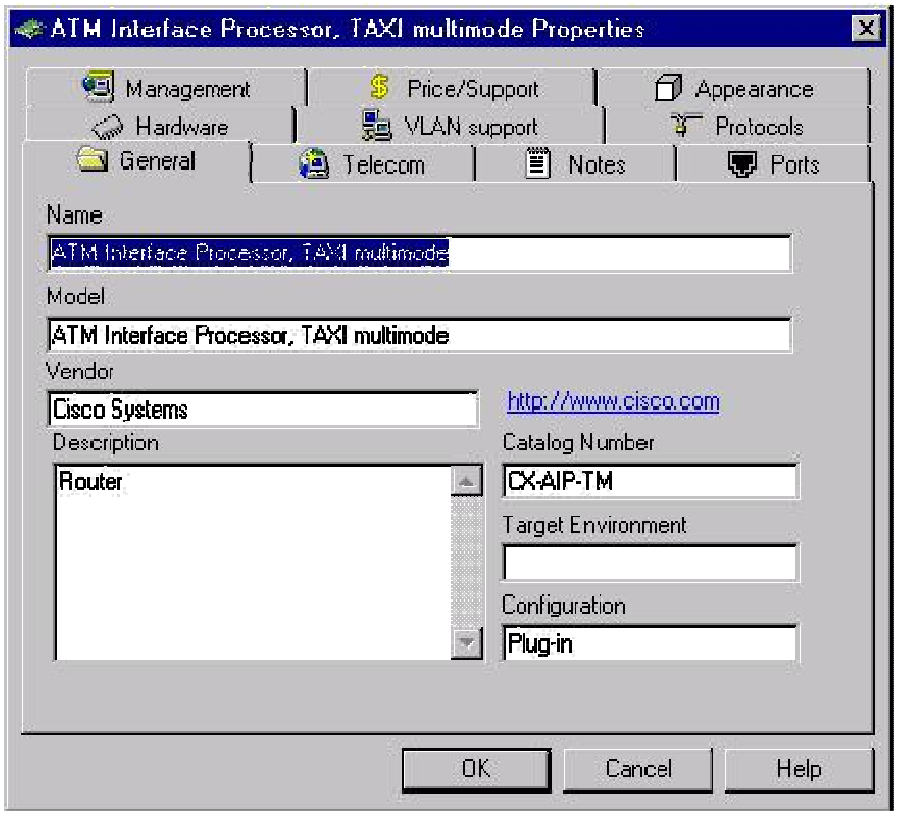


Рис.5.

Пройдите по закладкам и ознакомьтесь с содержащейся и возможной информацией о выбранном устройстве.

Все устройства, имеющиеся в базе данных Net Cracker, из браузера оборудования (страница Devices) можно перетаскивать в рабочее поле своего проекта, удерживая левую кнопку мыши. При этом курсор приобретает вид.

Устройства, размещенные в проекте должны быть соединены линиями связи.Net Cracker позволяет установить цвет линий в зависимости от используемого в проекте конкретного типа канала связи.

В главном меню View Media Colors и установить свои цвета для каждо-го типа канала связи (Рис.6).

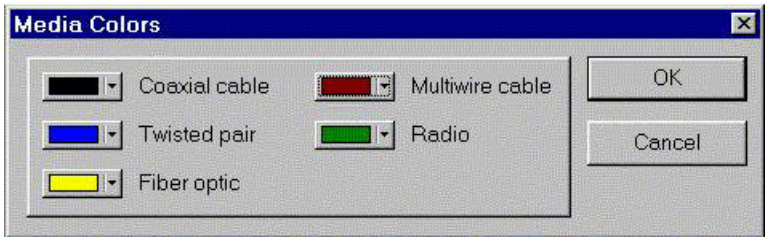


Рис.6.

Соединение устройств

Устройства соединяются с помощью мастера соединений "Link Assistant". Порядок соединения таков:

Выбрать в панели инструментов инструмент "Link devices":

Убедиться, что модули (компьютеры, коммутаторы, хабы), которые вы планируете соединить, имеют совместимые сетевые порты, например,100BASE-T.

Щелкнуть левой кнопкой мыши сначала по модулю-источнику трафика, затем по модулю-приемнику трафика

Нажать в диалоге "Link Assistant" на кнопку "Link", а также задать тип, длину и прочие характеристики среды.

Закрыть диалог нажав на кнопку "Close"

Задание трафика

При задании трафика нужно учитывать процессорные возможности компьютера. Так, при 30 потоках трафика и включенной анимации, для устойчивой работы программы требуется процессор не ниже Celeron-800. Проверьте конфигурацию своего компьютера: My Computer Properties. Немного облегчить задачу для компьютера можно отменив визуализацию передаваемых данных: Global Data Flow Uncheck All Close. При этом сохраняется возможность наблюдать результаты моделирования, получаемые через индикаторы статистики.

Трафик в моделируемой сети задается с помощью мастера, вызываемого кнопкой тулбара "Set traffic". Порядок задания трафика таков:

1. Выбрать в панели инструментов инструмент "Set traffic":

2.Щелкнуть левой кнопкой мыши сначала по модулю-источнику трафика, затем по модулю-приемнику трафика.

3.Наведите указатель мыши на один из стандартных профилей трафиков, например, "InterLAN traffic". Затем щелкните правой кнопкой мыши и в контекстном меню выберите данный профиль трафика (пункт Select).

При выборе профиля можно изменять характеристики профиля (кнопка Edit), задавая статистику размеров дейтаграмм "Transaction size", статистику моментов прихода дейтаграмм, пауз "Time between transactions", а также протокол уровня приложения "Application Layer Protocol".

5. Посмотрите на определенные Вами потоки данных в сети Global Data Flow. Здесь же можно отредактировать (в том числе и удалить) свойства потока и профилей трафиков.

6. При выборе трафика клиент-сервер, например, профиля трафика почтового клиента "E-mail (POP)", установите серверное приложение (в данном примере – почтовый сервер). Для этого, в браузере оборудования (закладка Devices) найдитегруппу "Network and Enterprise software". Затем перенеситеиконку "E-mail server" методом Drag-and-Drop на компьютер-сервер.

После такой установки программного обеспечения будет возможно назначать клиент-серверные трафики. Добавить другие виды серверного трафика можно в свойствах программного обеспечения сервера:

Контекстное меню компьютера Configuration Контекстное меню серверного программного обеспечения Properties Закладка Traffic

При назначении клиент-серверного трафика, можно изменять характеристики ответов сервера, задавая статистику размеров дейтаграмм "Transactionsize", статистику моментов прихода дейтаграмм, пауз "Time between trans-actions", а также протокол уровня приложения "Application Layer Protocol".

В процессе разработки текущего варианта проекта сети мы можем получить в Net Cracker отчеты о составе проекта. Например, Tools menu Reports Bill of Material позволяет получить отчет о номенклатуре оборудования, входящего в проект сети, ценах каждой единицы оборудования, общей цены проекта.

Tools menu Reports Device Summary позволяет получить отчет-спецификацию всех единиц оборудования.

Также подобные спецификации можно сгенерировать и по отдельным классам оборудования (например, Workstations, Servers, Hubs, и т. д.).

Полученные таким образом отчеты можно распечатать или сохранить в файл, воспользовавшись панелью меню по работе с отчетами (рис.7)

Рис.7.

При выборе опции сохранить появляется окно Export (рис.8), в котором можно определить формат сохраняемого отчета и место его хранения (файл на диске или отправка по почте).

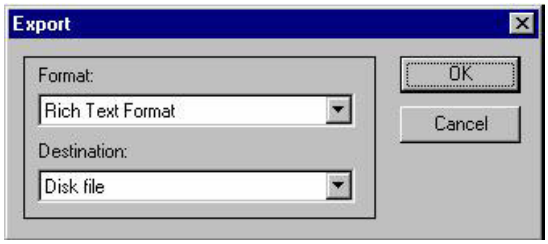


Рис.8.

Закройте проект Techno.net, выбрав File □ Close. В появившемся диалоговом окне с вопросом you want to save the file? Дайте ответ NO.

Задание для индивидуального выполнения

Рассмотрим возможности Net Cracker в отношении динамического моделирования сети. Откройте файл – пример проекта Router.net

Нажмите кнопку “старт”  на панели управления. 

Вы увидите следующую схему (Рис.9):

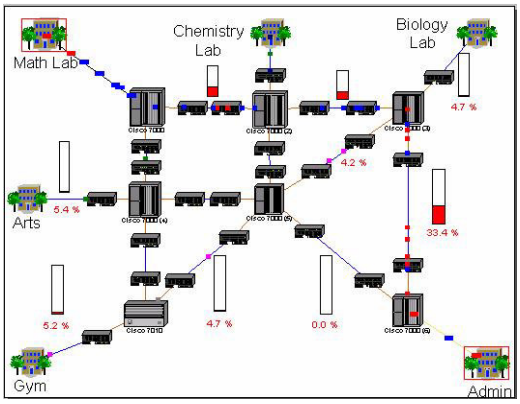


Рис.9.

Для изменения параметров анимации нажмите кнопку Animation Setup

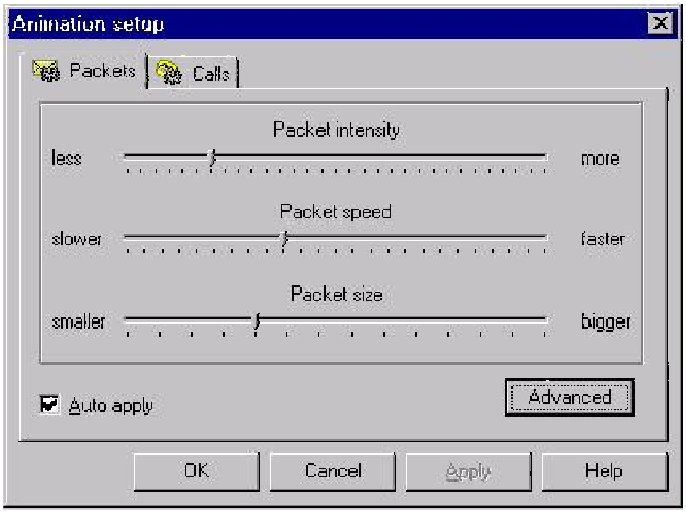


Рис.10

Измените параметры и нажмите на кнопу OK. Оцените изменения в статистике работы сети, показанные в проекте.

Рассмотрим работу сети на более подробном уровне. Для этого щелкните левой кнопкой мыши на открытом проекте, на здании отмеченном как MathLab. Перемещаться по иерархии сети можно и на закладке браузера оборудования «Project Hierarchy».

2.10 Лабораторная работа № 12, 13 (4 часа)

Тема: «Построение сети Ethernet»

2.10.1 Цель работы: изучить базовую технологию локальных сетей – Ethernet. Приобрести навыки проектирования сложной вычислительной сети для организации, имеющей несколько филиалов, расположенных на достаточном расстоянии друг от друга.

2.10.2 Задачи работы:

1. Изучить технологию Ethernet;
2. Ознакомиться с методом доступа CSMA/CD;
3. Рассмотреть оптоволоконный Ethernet;
4. Ознакомиться с доменом коллизий.

2.10.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.10.4 Описание (ход) работы:

В 1980 г. Институт инженеров по электротехнике и радиоэлектронике (InstituteofElectricalandElectronicsEngineers — IEEE) организовал комитет 802, в состав которого вошли рабочие и исследовательские группы, занимающиеся стандартизацией локальных сетей. Результатом их работы стал перечень стандартов, регламентирующих проектирование локальных сетей:

• IEEE 802.1 — стандарты, относящиеся к управлению сетями;

• IEEE 802.2 — общий стандарт управления логическим соединением (LogicalLinkControl — LLC) и управления доступом к среде (MediaAccessControl — MAC);

• IEEE 802.3, 802.4, 802.5 — стандарты, определяющие управление доступом к среде передачи данных (Ethernet, FDDI, Token Ring);

• IEEE 802.6 – стандарт для городских сетей;

• IEEE 802.11 – стандарт беспроводных технологий передачи данных;

• IEEE 802.12 – стандарт, определяющий технологию передачи данных с методом

доступа "приоритет запросов".

Технология Ethernet

Ethernet - это самый распространенный на сегодняшний день стандарт локальных сетей. В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации:

- 10Base-5;
- 10Base-2;
- 10Base-T;
- 10Base-FL;
- 10Base-FB;
- Fast Ethernet;
- Gigabit Ethernet.

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

Все виды стандартов Ethernet (в том числе Fast Ethernet и Gigabit Ethernet) используют один и тот же метод разделения среды передачи данных - метод CSMA/CD.

Метод доступа CSMA/CD

В сетях Ethernet используется метод доступа к среде передачи данных, называемый *методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD)*.

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

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

При описанном подходе возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общему кабелю. Для уменьшения вероятности этой ситуации непосредственно перед отправкой кадра передающая станция слушает кабель (то есть принимает и анализирует возникающие на нем электрические сигналы), чтобы обнаружить, не передается ли уже по кабелю кадр данных от другой станции. Если *опознается несущая (carrier-sense, CS)*, то станция откладывает передачу своего кадра до окончания чужой передачи, и только потом пытается вновь его передать. Но даже при таком алгоритме две станции одновременно могут решить, что по шине в данный момент времени нет передачи, и начать одновременно передавать свои кадры. Говорят, что при этом происходит *коллизия*, так как содержимое обоих кадров сталкивается на общем кабеле, что приводит к искажению информации.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется *обнаружение коллизии (collision detection, CD)*. Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети, ситуация коллизии усиливается посылкой в сеть станциями, начавшими передачу своих кадров, специальной последовательности битов, называемой *jam-последовательностью*.

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение случайного интервала времени, а затем может снова сделать попытку передачи кадра (рисунок 6.1).

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

Между двумя последовательно передаваемыми по общей шине кадрами информации должна выдерживаться пауза в 9.6 мкс; эта пауза нужна для приведения в исходное состояние сетевых адаптеров узлов, а также для предотвращения монопольного захвата среды передачи данных одной станцией.

При обнаружении коллизии станция выдает в среду специальную 32-х битную последовательность (jam-последовательность), усиливающую явление коллизии для более надежного распознавания ее всеми узлами сети.

После обнаружения коллизии каждый узел, который передавал кадр и столкнулся с коллизией, после некоторой задержки пытается повторно передать свой кадр. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой. Такой алгоритм выбора величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть при ее высокой загрузке.

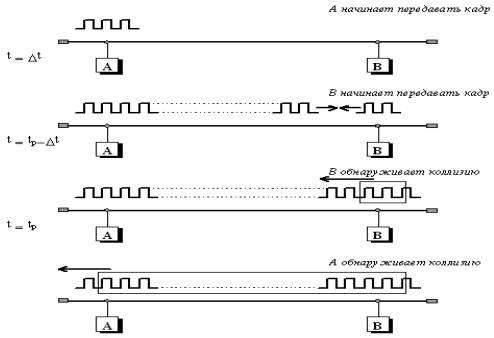


Рисунок 1 - Схема возникновения коллизии в методе случайного доступа CSMA/CD (tp - задержка распространения сигнала между станциями A и B)

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. Именно для этого минимальная длина поля данных кадра должна быть не менее 46 байт. Длина кабельной системы выбирается таким образом, чтобы за время передачи кадра минимальной длины сигнал коллизии успел бы распространиться до самого дальнего узла сети. Поэтому для скорости передачи данных 10 Мб/с, используемой в стандартах Ethernet, максимальное расстояние между двумя любыми узлами сети не должно превышать 2500 метров. Независимо от реализации физической среды, все сети Ethernet должны удовлетворять двум ограничениям, связанным с методом доступа: максимальное расстояние между двумя любыми узлами не должно превышать 2500 м; в сети не должно быть более 1024 узлов.

Оптоволоконный Ethernet

В качестве среды передачи данных 10 мегабитный Ethernet использует оптическое волокно. Оптоволоконные стандарты в качестве основного типа кабеля рекомендуют достаточно дешевое оптическое волокно, обладающее полосой пропускания 500-800 МГц при длине кабеля 1 км.

Функционально сеть Ethernet на оптическом кабеле состоит из тех же элементов, что и сеть стандарта 10Base-T - сетевых адаптеров, многопортового повторителя и отрезков кабеля, соединяющих адаптер с портом повторителя. Как и в случае витой пары, для соединения адаптера с повторителем *используются два* оптоволокна - одно соединяет выход T_x адаптера со входом R_x повторителя, а другое - вход R_x адаптера с выходом T_x повторителя.

Стандарт FOIRL (Fiber Optic Inter-Repeater Link) представляет собой первый стандарт комитета 802.3 для использования оптоволокна в сетях Ethernet. Он гарантирует длину оптоволоконной связи между повторителями до 1 км при общей длине сети не более 2500 м. Максимальное число повторителей между любыми узлами сети - 4. Максимального диаметра в 2500 м здесь достичь можно, хотя максимальные отрезки кабеля между всеми 4 повторителями, а также между повторителями и конечными узлами недопустимы - иначе получится сеть длиной 5000 м.

Стандарт 10Base-FL представляет собой незначительное улучшение стандарта FOIRL. Увеличена мощность передатчиков, поэтому максимальное расстояние между узлом и концентратором увеличилось до 2000 м. Максимальное число повторителей между узлами осталось равным 4, а максимальная длина сети - 2500 м.

Стандарт 10Base-FB предназначен только для соединения повторителей. Конечные узлы не могут использовать этот стандарт для присоединения к портам концентратора. Между узлами сети можно установить до 5 повторителей 10Base-FB при максимальной длине одного сегмента 2000 м и максимальной длине сети 2740 м.

Как и в стандарте 10Base-T, оптоволоконные стандарты Ethernet разрешают соединять концентраторы только в древовидные иерархические структуры. Любые петли между портами концентраторов не допускаются.

Домен коллизий

В технологии Ethernet, независимо от применяемого стандарта физического уровня, 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 коллизия возникла. Сеть Ethernet, построенная на повторителях, всегда образует один домен коллизий. Домен коллизий соответствует одной разделяемой среде. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий.

Задание

Спроектировать вычислительную сеть для организации, имеющей несколько филиалов в различных городах. Используется 4 филиала в 4 населенных пунктах. Число компьютеров в каждом филиале - 5-5-8-6. Расстояние между сегментами -25-20-25-20 км.

При проектировании использовать максимально возможное разнообразие коммуникационного оборудования. На схеме указать типы использованных сред передачи данных.

Определить несколько маршрутов продвижения пакета из одного узла в другой, составить таблицу маршрутизации.

Спроектировать сеть для организации, которая состоит из нескольких филиалов (варианты представлены в таблице А.1).

Таблица А.1

ВАРИАНТ	Количество филиалов	Число компьютеров в каждом филиале	Количество населенных пунктов	Расстояние между сегментами, км
1	7	(12)-(24-5)	6	250-(0,4)

2	8	(10-10)-(24-11)	6	(1,8)-120-(0,15)
3	9	2-3-12-8-16	5	0,2-1,5-0,13-0,4
4	7	12-26-18	7	18-23
5	8	5-8-4-6	8	250-500-750
6	6	18-24	6	530
7	8	(10)-(8-7)-(29)	7	123-(0,2)-12
8	7	(8-19)-(23)	6	0,2-300
9	9	(12-12-14)-(8-12)	6	(0,3-0,4)-(0,25)
10	8	5-5-8-6	8	25-20-25-20
11	7	12-8-14	7	21-10
12	6	36-8	6	12-5
13	8	(12-2-3)-(15)	6	(1,8-0,4-0,9)-13
14	7	(10-8)-(16-14)	6	14-3
15	6	12-60	6	126
16	9	12-2-8-24-10	5	2-5-12-0,8
17	8	(11-5)-(3-12)	6	8-17
18	7	14-14-8	5	250-300
19	6	24-36	5	12
20	7	9-21-3	7	45-12-100

Необходимо добиться максимальной эффективности использования сети по критерию цена-качество-скорость.

2.11 Лабораторная работа № 14, 15 (4 часа)

Тема: «Модуляция»

2.11.1 Цель работы: изучить методы амплитудной, фазовой и частотной модуляции, принципы амплитудной и частотной манипуляции, принципы импульсной и цифровой модуляции.

2.11.2 Задачи работы:

1. Изучить методы модуляции;
2. Изучить принципы модуляции.

2.11.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.11.4 Описание (ход) работы:

Модуляция сигналов позволяет выполнить преобразование сигналов с целью повышения эффективности и помехоустойчивости процесса передачи информации. В большинстве случаев методы модуляции основываются на управлении параметрами сигналов в соответствии с информационным сообщением. При модуляции сигналов изменяется их форма и спектральные характеристики. Особенности формирования спектров сигналов имеют важное значение для систем связи и телекоммуникаций.

Сообщения передаются при помощи сигналов. В простейшем случае сообщение может заключаться в наличии (отсутствии) принятого сигнала. При этом требуется решать задачу *обнаружения* сигнала. Во многих случаях вид передаваемых сигналов заранее известен и приём сообщения состоит в том, чтобы определить, какой из возможных сигналов был передан. Тогда задача состоит в *различении* сигналов. Если сигналы отличаются значениями их параметров, которые считаются постоянными в течениии некоторого интервала, то необходимо получать *оценки параметров* сигнала. Сообщение может содержаться в изменениях параметров, т.е. в их мгновенных (локальных) значениях. Тогда для получения сообщения нужно выполнить *фильтрацию параметров* сигнала. Задача фильтрации, как правило, является более сложной, чем оценивание параметров.

Управление информационным параметром сигнала в соответствии с передаваемым сообщением называют *модуляцией*.

Информационный сигнал (сообщение) обозначим q(x), сигнал-переносчик, параметр которого изменяется в соответствии с сообщением, обозначим *s(x)*. При модуляции выполняется преобразование этих двух сигналов в один модулированный сигнал x(x) в соответствии с уравнением

$$\xi(x) = \mathrm{M}\{s(x), \theta(x)\}, \quad (1)$$

где $\mathrm{M}\{.\}$ – оператор, определяемый видом модуляции. Для выделения сообщения q(x) на приёмной стороне необходимо выполнить обратное преобразование (демодуляцию), т.е.

$$\theta(x) = \mathrm{M}^{-1}\{\xi(x)\}. \quad (2)$$

В зависимости от вида, функциональной формы и числа параметров сигнала-переносчика *s(x)* и информационного сигнала q (x) варьируются свойства различных методов модуляции, а именно, вид и ширина спектра сигнала x(x), устойчивость к воздействию помех и т.д.

Если информационный параметр сигнала-переносчика изменяется непрерывно, то методы модуляции являются *непрерывными* (распространены, например, методы

амплитудной, фазовой и частотной непрерывной модуляции гармонического сигнала-переносчика).

В качестве сигнала-переносчика часто используют периодическую последовательность импульсов, тогда модуляцию называют *импульсной* (например, при изменении амплитуды или частоты импульсов по закону $q(x)$ имеет место амплитудно-импульсная или частотно-импульсная модуляция соответственно).

Информационный параметр может принимать счётное число значений, при этом модуляцию называют *дискретной*. К дискретным видам модуляции относятся, например, амплитудная, частотная и фазовая *манипуляции*. Если значения параметра закодированы и передаются в цифровой форме, то соответствующие виды модуляции носят название *цифровой* модуляции. Наиболее распространенным видом цифровой модуляции является импульсно-кодовая модуляция, когда значения сигнала в дискретных точках кодируют в цифровой форме.

При создании систем передачи сигналов основными задачами являются разработка методов и математических моделей, определяющих оптимальные режимы модуляции-демодуляции с точки зрения повышения скорости, достоверности и помехозащищённости передачи информации.

При классификации видов модуляции принимают в расчёт вид, характер информационного сигнала и сигнала-переносчика: детерминированный процесс, случайный стационарный процесс, нестационарный процесс и т.д. Детерминированные сигналы определяются их амплитудными и фазовыми спектрами на основе свойств рядов Фурье и преобразования Фурье (разд. 1.5.). В теории информации и передачи сигналов особое место занимают стохастические сигналы, являющиеся реализациями случайных процессов с заданными характеристиками – корреляционными функциями и спектральными плотностями.

Если вид информационного сигнала, сигнала-переносчика и характеристики линии связи заданы, то основной задачей является *оптимальный приём* сигналов. Задача оптимального приёма, как правило, сводится к задаче различения сигналов по заданному критерию в условиях помех (задача обнаружения рассматривается как различение смеси сигнала и помехи от помехи, когда сигнал отсутствует).

Задачи приёма сообщений подразделяют на два класса – когерентный и некогерентный приём, соответственно при наличии и отсутствии синхронизации в канале передачи информации. Методы когерентного (синхронного) приема, как правило, более просты и надёжны. Методы некогерентного (асинхронного) приёма обеспечивают более высокое быстродействие, однако более сложны в реализации.

Теория оптимального приёма сигналов является одним из важнейших разделов статистической радиотехники и теории связи.

Методы амплитудной, фазовой и частотной модуляции

Амплитудная, фазовая и частотная модуляция гармонических сигналов-переносчиков получили наиболее широкое распространение в радиовещании и системах связи.

Амплитудная модуляция

Амплитудно-модулированный (АМ) сигнал в общем случае определяется выражением

$$\xi(x) = [1 + m\Theta(x)]\, s(x), \quad (3)$$

где q(x) – информационный (модулирующий) сигнал, *s(x)* – сигнал-переносчик, m – коэффициент модуляции.

Спектр сигнала (3) можно найти с использованием свойств преобразования Фурье (см. разд. 1.5) в форме

$$\Xi(u) = F\{\xi(x)\} = S(u) + m\, S(u) * \Theta(u), \quad (4)$$

где $S(u) = F\{s(x)\},\ \Theta(u) = F\{\Theta(x)\}.$

Формирование спектра (4) иллюстрируется на рис. 1 и 2.

При гармоническом модулирующем сигнале (рис. 1) его спектр, как и спектр сигнала-переносчика, представляет собой две дельта-функции. Свертка спектров *S(u)* и Q (u) приводит к переносу спектра Q(u) на более высокую (так называемую *несущую*) частоту $\pm u_0$.

Если модулирующий сигнал имеет сложную форму и, следовательно, протяженный спектр (рис. 2), образованный множеством пар дельта-функций с различными положениями на частотной оси, то в результате переноса спектра на несущую частоту $\pm u_0$ образуются соответствующие спектральные порядки. В силу свойств частотной симметрии преобразования Фурье можно показать, что вся полезная информация содержится в спектральном порядке в окрестности частоты u_0.

Демодуляцию АМ сигнала осуществляют путём выделения огибающей сигнала-переносчика при его детектировании и фильтрации нижних частот на выходе детектора. Ширина полосы пропускания фильтра должна соответствовать ширине спектра Q(u) (рис. 2), чтобы обеспечить минимальные спектральные искажения восстановленного сигнала.

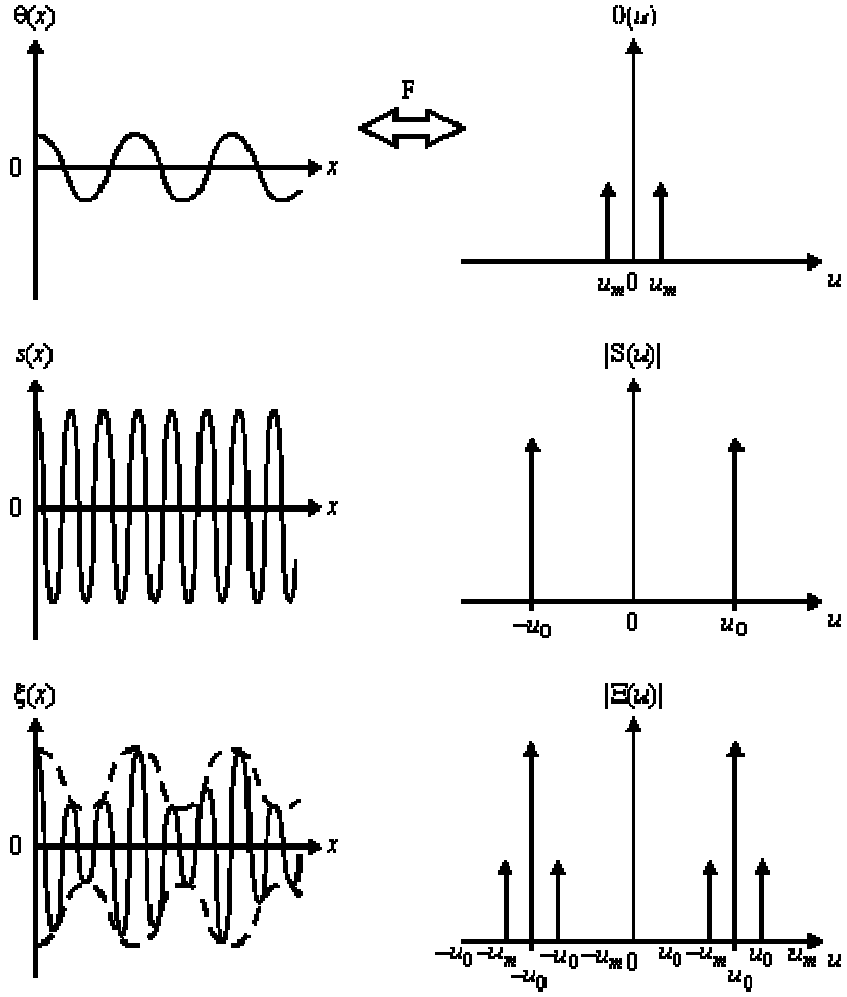


Рис. 1. Спектр АМ сигнала с гармонической модуляцией

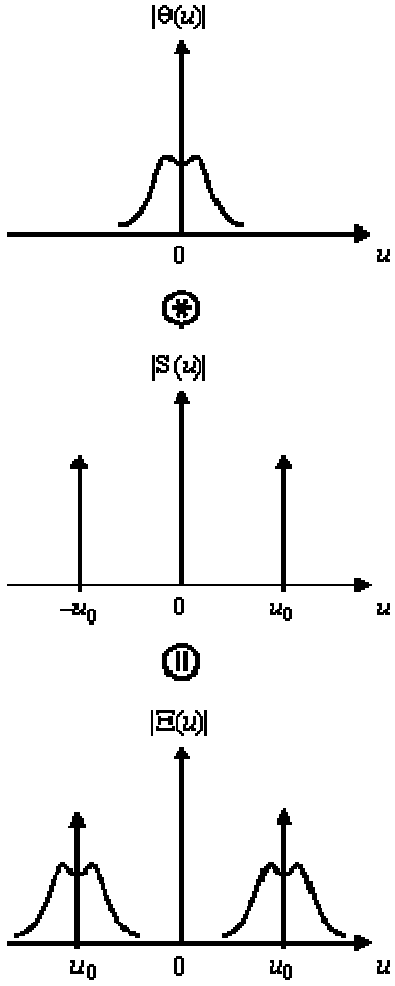


Рис. 2. Спектр сложного АМ сигнала

Фазовая модуляция

Фазомодулированный (ФМ) сигнал имеет постоянную амплитуду, фаза сигнала изменяется пропорционально информационному сигналу, а именно

$$\xi(x) = A\cos[2\pi u_0 x + m\Theta(x)], \quad (5)$$

где u_0 - несущая частота, *m* – индекс фазовой модуляции.

Пусть модулирующий сигнал является гармоническим, $\Theta(x) = \cos(2\pi u_m x)$, и индекс модуляции $m << 1$. При этом выражение (5) можно переписать в виде

$$\xi(x) = A\cos[2\pi u_0 x + m\cos(2\pi u_m x)] \approx$$
$$\approx A\cos(2\pi u_0 x) - mA\sin(2\pi u_0 x)\cos(2\pi u_m x), \quad (6)$$

учитывая, что при $y \to 0$ $\cos y \approx 1, \sin y \approx y$. После преобразования второго слагаемого в (6) получим

$$\xi(x) \approx A\cos(2\pi u_0 x) - (mA/2)\sin 2\pi(u_0 + u_m)x - (mA/2)\sin 2\pi(u_0 - u_m)x. \quad (7)$$

Спектр ФМ-сигнала с малым индексом модуляции показан на рис. 3.

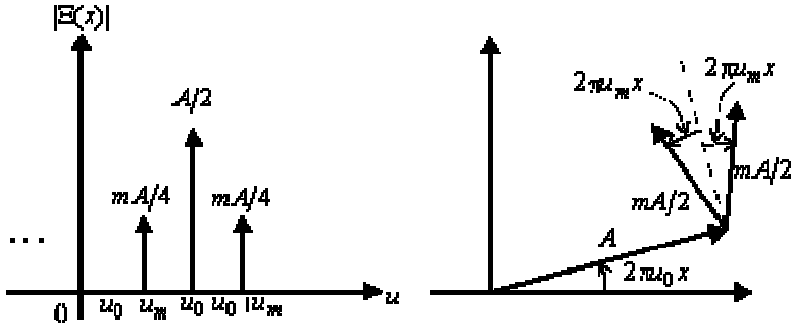


Рис. 3. Спектр и векторная диаграмма для ФМ сигнала при *m <<1*

Величины спектральных составляющих идентичны величинам спектральных составляющих сигнала с синусоидальной АМ, однако фазовые соотношения между несущей и боковыми составляющими различны. Эти фазовые соотношения более детально показаны графически на векторной диаграмме в правой части рис. 3. Меньшие векторы медленно вращаются в противоположных направлениях вокруг быстро вращающегося большого вектора, а x (*x*)представляет собой проекцию суммы векторов на горизонтальную ось. Однако в отличие от случая АМ сигнала сумма меньших векторов всегда перпендикулярна большему вектору. При этом, если векторы боковых составляющих малы (*m << 1)*, длина суммарного вектора близка по величине амплитуде несущей *A*, но результирующий вектор вращается с переменной скоростью.

Фазовые соотношения в данной векторной диаграмме указывают простой способ генерирования ФМ сигналов с малым индексом модуляции (рис. 2.4) при произвольном модулирующем сигнале q (*x*).

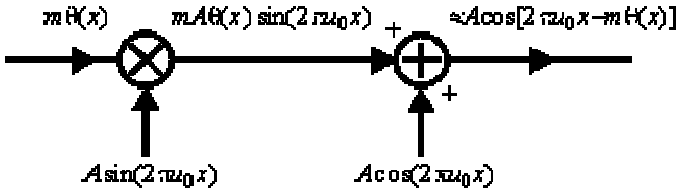


Рис. 4. Структурная схема ФМ модулятора при *m <<1*

Частотная модуляция

При частотной модуляции изменяется мгновенная (локальная) частота *u(x)* сигнала-переносчика *s(x)* в соответствии с информационным сигналом q(*x*), а именно

$$\xi(x) = A\cos[2\pi u(x)x], \quad (8)$$

где

$$u(x) = u_0 + \int_{-\infty}^{x} \theta(\chi)\, d\chi. \quad (9)$$

При синусоидальной ЧМ модулирующий сигнал имеет вид

$$\theta(x) = -a\sin(2\pi u_m x), \quad (10)$$

откуда

$$u(x) = u_0 + \int_{-\infty}^{x} \theta(x)\,dx = u_0 + (a/2\pi u_m)\cos(2\pi u_m x). \quad (11)$$

Сравнение (6) и (8) с учётом (11) показывает идентичность ФМ и ЧМ при синусоидальной модулирующей функции и индексе модуляции

$$|m| = a/2\pi u_m .$$

Значение *а*представляет собой максимальную *девиацию* мгновенной угловой частоты относительно несущей угловой частоты $2\pi u_0$.

Простейший демодулятор для ЧМ сигналов или *частотный дискриминатор* представляет собой резонансный контур, настроенный, например, ниже несущей частоты (рис. 5). Изменения мгновенной частоты во входном модулированном сигнале преобразуются в изменения амплитуды сигнала на выходе резонансного контура. Эти амплитудные изменения нетрудно выделить при помощи обычного детектора огибающей.

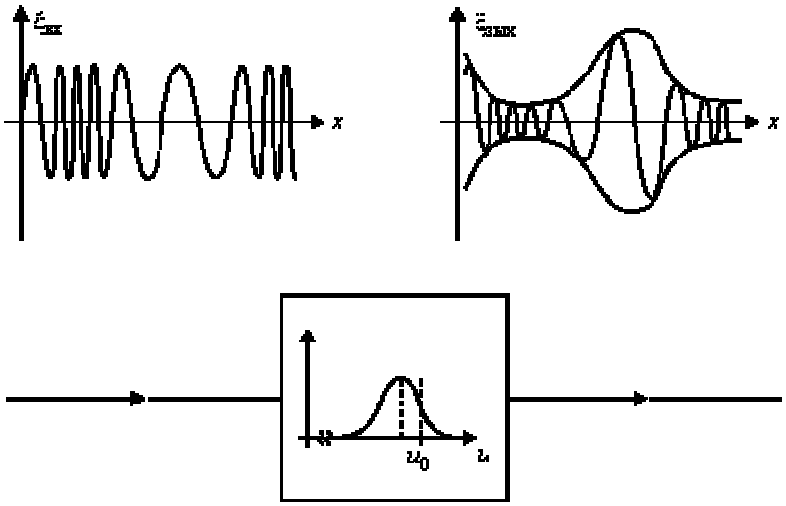


Рис. 5. Преобразование изменений частоты в изменение амплитуды при помощи резонансной цепи

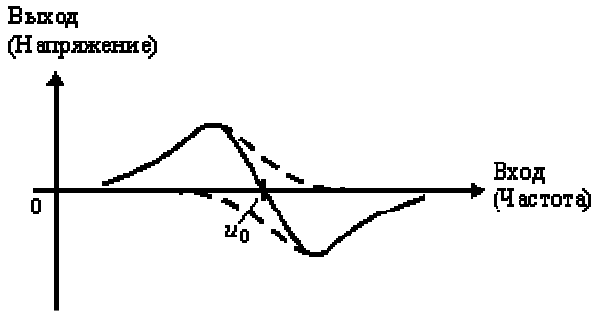


Рис. 6. Характеристика дискриминатора, полученная с помощью пары резонансных контуров

Ограниченный диапазон линейности такого дискриминатора можно расширить, применив пару контуров, один из которых настроен соответственно выше, а другой ниже частоты несущей. Выходные сигналы на выходе этих контуров раздельно детектируются и после этого вычитаются, образуя полную характеристику дискриминатора, показанную на рис. 6. Выходной сигнал в дискриминаторах такого типа изменяется по амплитуде при вариациях как частоты, так и амплитуды входного сигнала.

В реальных системах неконтролируемые изменения амплитуды в ЧМ-сигнале вызываются шумами, помехами, “замираниями” радиоволн и другими факторами. В связи с этим на входе дискриминаторов необходимо включать*ограничитель*, который представляет собой нелинейное устройство с характеристикой, показанной на рис. 7. Ограничитель совместно с включенным на его выходе резонансным усилителем практически устраняет амплитудные изменения огибающей узкополосного сигнала, сохраняя при этом фазовые изменения.

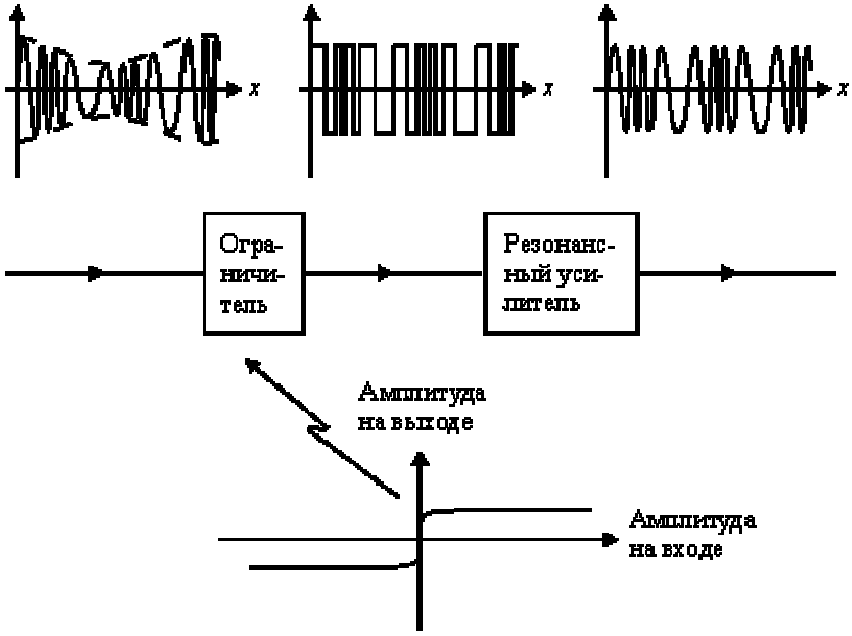


Рис. 7. Совместная работа ограничителя и резонансного усилителя

На рис. 8 показана полная структурная схема типового ЧМ приемника.

Усилитель высокой частоты (УВЧ) усиливает принятый сигнал, внутренний гетеродин (генератор) вырабатывает гармонический “опорный” сигнал, который перемножается в смесителе с принятым сигналом. В результате формируется сигнал на промежуточной частоте, которая является постоянной при синхронной перестройке частот настройки УВЧ и гетеродина.

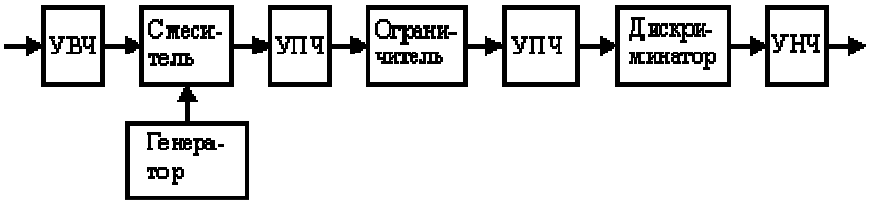


Рис.8. Функциональная схема ЧМ приемника

Усилитель промежуточной частоты УПЧ обеспечивает высокий коэффициент усиления сигнала. Усиленный сигнал после ограничителя поступает на второй УПЧ, выполняющий функции резонансного усилителя в схеме рис. 7. Частотный дискриминатор выделяет изменения частоты сигнала, которые в форме низкочастотного сигнала поступают на вход усилителя низкой частоты УНЧ.

Принципы амплитудной и частотной манипуляции

Манипуляция относятся к дискретным методам модуляции, в которых информационный параметр принимает счётное число значений.

Амплитудная манипуляция

При амплитудной манипуляции (АМн) информационным параметром является амплитуда сигнала-переносчика, которая изменяется скачкообразно под действием модулирующего сигнала.

Рассмотрим особенности анализа АМн сигнала для случая, когда в роли переносчика выступает гармоническое колебание $s(x) = A_0 \sin(2\pi u_0 x + \varphi_0)$, а модулирующим сигналом является периодическая последовательность модулирующих импульсов

$$\theta(x) = \begin{cases} 1, & 2i\Delta x < x < (2i+1)\Delta x, \\ -1, & (2i+1)\Delta x < x < 2(i+1)\Delta x, \ i = 0, 1, 2..., \end{cases}$$

где Δx - длительность импульсов, $T = 2\Delta x$ - период следования импульсов. Аналитически АМн сигнал определяется выражением

$$\xi(x) = 0{,}5A_0[1 + m\theta(x)]\sin(2\pi u_0 x + \varphi_0). \quad (12)$$

В рассматриваемом примере амплитуда манипулированного сигнала принимает два значения:

$$A = \begin{cases} 0{,}5A_0(1+m), & 2i\Delta x < x < (2i+1)\Delta x, \\ 0{,}5A_0(1-m), & (2i+1)\Delta x < x < 2(i+1)\Delta x, \ i = 0, 1, 2, \ldots \end{cases}$$

Обычно коэффициент модуляции m при АМн выбирается равным единице, поэтому амплитуда модулированного сигнала изменяется скачком в точках $x = i\Delta x, \ i = 0, 1, 2, \ldots$ и принимает два значения A_0 и 0.

На рис. 9 показаны временные диаграммы модулирующего $\theta(t)$ и манипулированного $\xi(t)$ сигналов.

Определим спектр амплитудно манипулированного сигнала (12). Представим модулирующий сигнал q(x) в виде ряда Фурье

$$\theta(x) = \frac{2}{\pi}\sum_{k=1}^{\infty}\frac{1-\cos k\pi}{k}\sin 2\pi k u_m x \quad , (13)$$

где $u_m = 1/T$. Подставив (13) в (12), получим

$$\xi(x) = A_0\left(\frac{1}{2} + \frac{1}{\pi}\sum_{k=1}^{\infty}\frac{1-\cos k\pi}{k}\sin 2\pi k u_m x\right)\sin(2\pi u_0 x + \varphi_0) =$$
$$= \frac{1}{2}A_0\sin(2\pi u_0 x + \varphi_0) + \frac{A_0}{2\pi}\sum_{k=1}^{\infty}\frac{1-\cos k\pi}{k}\cos(2\pi u_0 x - 2\pi k u_m x + \varphi_0) -$$
$$- \frac{A_0}{2\pi}\sum_{k=1}^{\infty}\frac{1-\cos k\pi}{k}\cos(2\pi u_0 x + 2\pi k u_m x + \varphi_0). \quad (14)$$

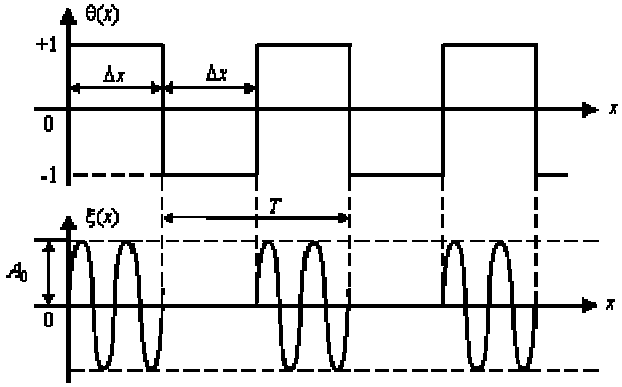


Рис. 9. Модулирующий и манипулированный сигналы.

На рис. 10 показан построенный в соответствии с выражением (14) спектр АМн сигнала. Огибающая спектра (штрихованная линия) представляет смещенный на частоту u_0 спектр одиночного видеоимпульса $h(x)$.

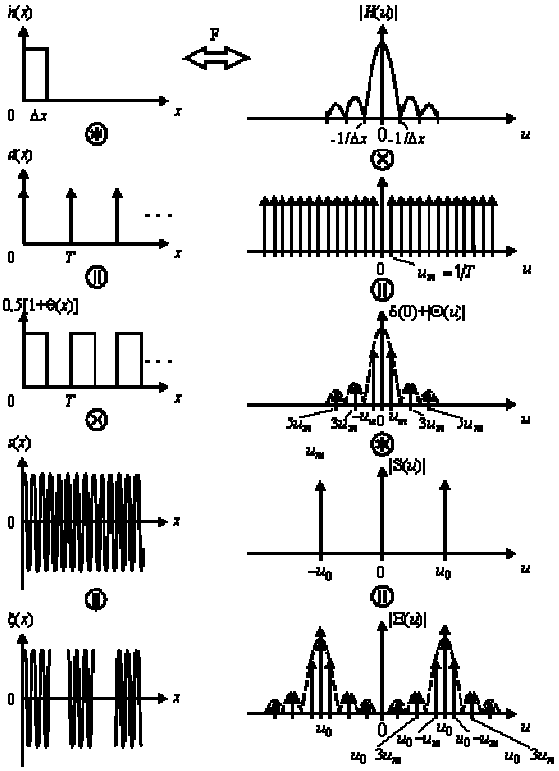


Рис. 10. Формирование спектра сигнала при амплитудной модуляции

Интервалы между спектральными линиями равны $u_м = 1/T$ (чётные гармоники равны нулю).

Отношение периода следования импульсов к их продолжительности называется *скважностью* импульсов $\eta = (T/\Delta x)$. Рассмотренный пример соответствует случаю h = 2. При других значениях скважности спектр сигнала может содержать также четные гармонические составляющие частоты $u_м$.

Частотная манипуляция

Сигнал с частотной манипуляцией (ЧМн) формируется в результате скачкообразного изменения частоты сигнала-переносчика, а именно, при манипуляции со скважностью h = 2 ЧМн сигнал внутри периода манипуляции определяется как

$$\xi(x) = \begin{cases} A\cos[(2\pi u_0 + \Delta u)x], & -T/4 < x < T/4, \\ A\cos[2\pi(u_0 - \Delta u)x](x - T/2), & T/4 < x < 3T/4, \end{cases}$$

где $2\Delta u$ - изменение частоты, T – период изменения частоты (рис 2.11).

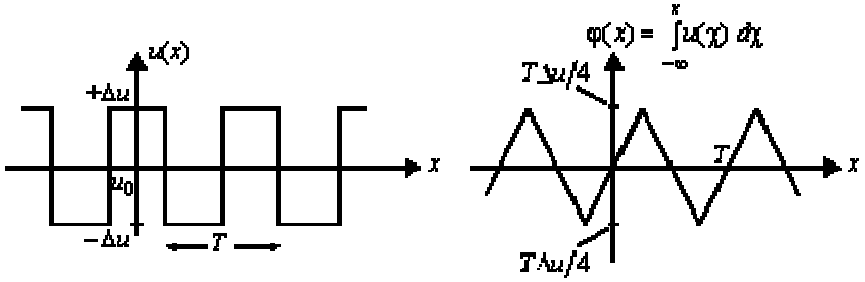


Рис. 11. Модулирующие функции частотно манипулированного сигнала

Частота сигнала мгновенно изменяется между двумя значениями на оси частот. Результирующий сигнал $\xi(x)$ можно рассматривать как суперпозицию двух модулированных прямоугольной последовательностью импульсов синусоидальных сигналов различной частоты, как показано на рис. 12. Спектр каждой из составляющих представляет собой спектр прямоугольного видеоимпульса с соответственно сдвинутой несущей частотой, как показано на рис. 13.

Согласно рис. 11, периодическая частотная манипуляция соответствует фазовой модуляции сигналом треугольной формы.

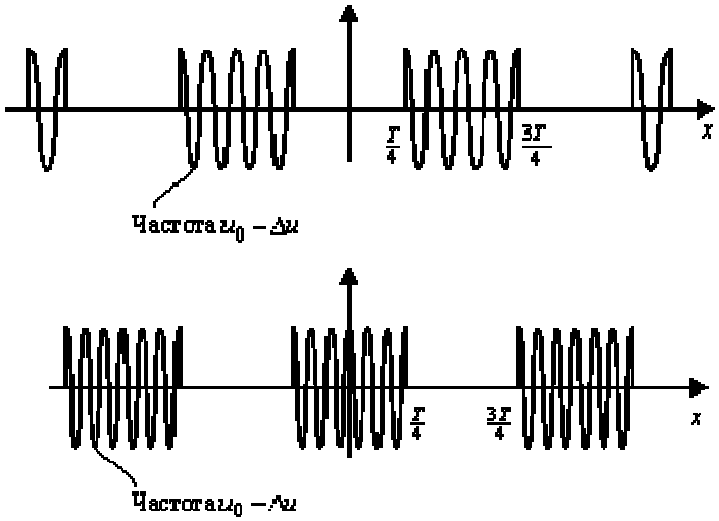


Рис. 12. Две составляющие частотно манипулированного сигнала

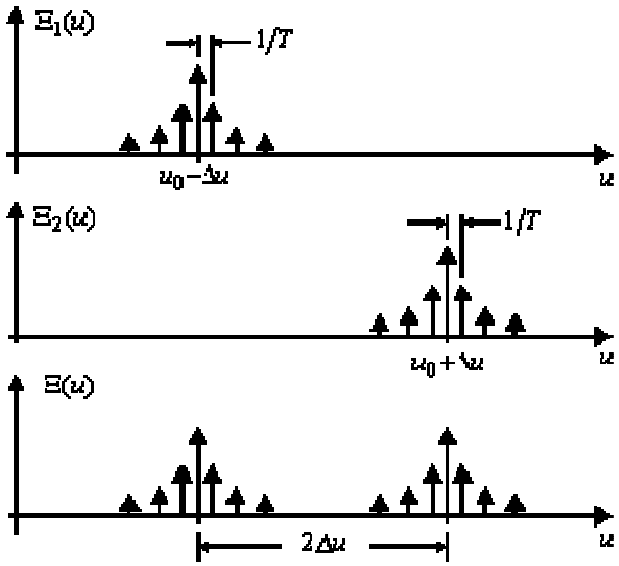


Рис. 13. Спектры частотно манипулированного сигнала

Во многих случаях при манипуляции модулирующие сигналы не являются периодическими и представляют собой случайные последовательности (соответствующие, например, последовательностям нулей и единиц при передаче информации). При этом характеристики сигналов определяются их корреляционными функциями и спектральными плотностями.

Принципы импульсной и цифровой модуляции

При импульсной модуляции в качестве сигнала-переносчика используется периодическая последовательность видеоимпульсов

$$s(x) = A_0 \sum_{i=-\infty}^{\infty} h(x - iT, \Delta x), \quad (15)$$

где A_0 – амплитуда импульсов, $h(x)$ – функция, описывающая одиночный импульс последовательности, T – период повторения импульсов, Δx - длительность одного импульса.

В качестве примера рассмотрим метод амплитудной импульсной модуляции (АИМ), когда амплитуда импульсов изменяется в соответствии с информационным сигналом $\theta(x)$, так что передаваемый сигнал определяется выражением

$$\xi(x) = A_0[1 + m\theta(x)] \sum_{i=-\infty}^{\infty} h(x - iT, \Delta x), \quad (16)$$

где m, как и ранее, – коэффициент модуляции. Временная диаграмма сигнала (16) показана на рис. 14.

Представим последовательность (15) в форме ряда Фурье

$$s(x) = \sum_{k=-\infty}^{\infty} a_k \exp(j2\pi k u_0 x), \quad (17)$$

где a_k – комплексные амплитуды, учитывающие амплитуды и начальные фазы отдельных гармоник, $u_0 = 1/T$ – частота следования видеоимпульсов.

В результате подстановки (17) в (16) и преобразования Фурье получим выражение для спектра АИМ сигнала в форме

$$\begin{aligned} \Xi(u) &= \int_{-\infty}^{\infty} \xi(x) \exp(-j2\pi u x) dx = \\ &= \int_{-\infty}^{\infty} [1 + m\theta(x)] \sum_{k=-\infty}^{\infty} a_k \exp[-j2\pi(u - ku_0)x]\, dx = \\ &= 2\pi \sum_{k=-\infty}^{\infty} a_k \delta(u - ku_0) + m \sum_{k=-\infty}^{\infty} a_k \int_{-\infty}^{\infty} \theta(x) \exp[-j2\pi(u - ku_0)x]\, dx. \end{aligned} \quad (18)$$

Первая сумма в (18) представляет спектр немодулированной последовательности (17). Вторая сумма показывает, что амплитудная модуляция вызывает появление возле каждой составляющей этого спектра боковых полос, повторяющих спектр узкополосного модулирующего сигнала. Поэтому спектр АИМ сигнала представляет упорядоченный набор спектров обычных АМ колебаний (см. рис. 2), в которых роль несущих выполняют гармоники (17) частоты следования видеоимпульсов (15).

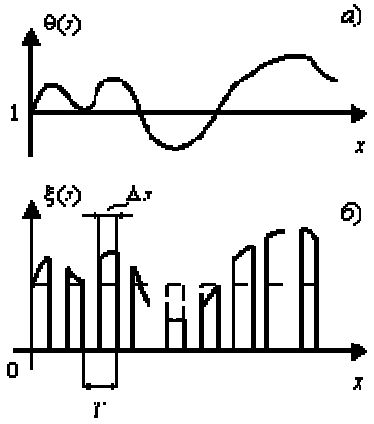


Рис. 14. Модулирующий сигнал (*а*) и АИМ сигнал (*б*)

Спектр АИМ сигнала показан на рис. 15 для случая, когда модулирующий сигнал $\theta(x)$ является узкополосным сигналом со средней частотой $u_м$.

Рассмотрение спектра АИМ сигнала позволяет сделать ряд практически важных выводов. Очевидно, что необходимо выбирать такую частоту повторения импульсов $u_{0min} \geq 2u_м$, при которой не происходит наложения спектров соседних боковых полос. Если это условие выполняется, можно выделить составляющие модулированного сигнала с помощью полосовых фильтров и фильтров нижних частот. Практически важной особенностью спектра АИМ сигнала является наличие около частоты $u = 0$ составляющих модулирующего сигнала (рис. 15). Следовательно, демодуляцию АИМ сигнала можно выполнить фильтром нижних частот без дополнительных преобразований. Фильтр должен пропускать частоты от 0 до $u_0 - u_м - u_M$, где u_M – максимальная частота в спектре модулирующего информационного сигнала.

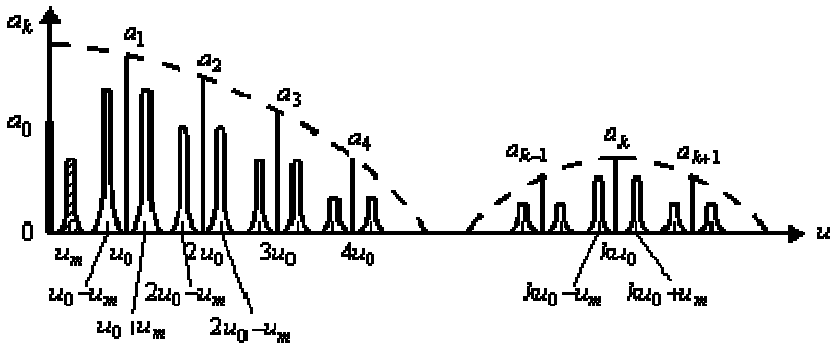


Рис. 15. Модуль спектра АИМ сигнала

Частоте u_0 соответствует период T. Большие интервалы между импульсами используются для размещения импульсов других каналов, например, при многоканальной передаче с временным разделением каналов. Длительность Δx импульсов определяет полосу пропускания каналов.

Часто АИМ сигнал используется как модулирующий сигнал для создания высокочастотных модулированных колебаний. Вначале формируют АИМ сигнал, затем полученный АИМ видеосигнал используют для модуляции непрерывного высокочастотного переносчика, имеющего частоту много большую, чем u_0. После таких преобразований спектр сигнала $\theta(x)$ переносится на частоту несущего высокочастотного колебания.

Цифровые методы модуляции

Цифровые виды модуляции используются для передачи кодированных сообщений дискретными методами. Сущность цифровой модуляции заключается в том, что передаваемый непрерывный сигнал дискретизируется во времени, квантуется по уровню и полученные отчеты, следующие в дискретные моменты времени, преобразуются в кодовые

комбинации. Полученной последовательностью кодовых видеосигналов модулируется высокочастотный сигнал-переносчик.

Следовательно, цифровые методы модуляции основаны на трех необходимых преобразованиях полезных непрерывных сигналов: дискретизации, квантовании и кодировании.

Достоинствами цифровых методов модуляции являются:

- слабое влияние неидеальности и нестабильности характеристик аппаратуры на качество передачи информации;
- высокая помехоустойчивость даже при использовании каналов с нестабильными характеристиками и большим уровнем шумов;
- возможность регенерации (восстановления) сигналов в узлах связи сетей, что значительно ослабляет эффект накопления искажений сигналов при передаче информации по линиям большой протяженности;
- универсальная форма представления сигналов для различных сообщений (речь, телевизионное изображение, дискретные данные, команды управления работой устройств связи и т.п.);
- низкая чувствительность к нелинейным искажениям в групповом тракте многоканальных систем;
- относительно простое согласование этих систем с компьютерами и электронными автоматическими телефонными станциями, что играет важную роль для построения сетей связи;
- возможность автоматизации передачи и обработки сигналов с помощью компьютеров.

Основными недостатками систем с цифровыми способами передачи сигналов являются: значительное расширение занимаемой полосы частот каналов, необходимость обеспечения точной синхронизации сигналов и построения аппаратуры для регенерации сигналов на линиях большой протяженности.

В настоящее время наибольшее распространение получили системы с импульсной кодовой модуляцей (ИКМ), в которых значение сигнала в дискретные моменты времени преобразуется в двоичные цифровые коды.

На рис. 16 показаны временные диаграммы сигналов в системе с ИКМ. На рис. 16,*а* представлены исходный непрерывный сигнал с ограниченным спектром и дискретизированный сигнал с интервалом дискретизации $T < 1/2u_M$, где u_M - верхняя частота спектра сигнала. На рис. 16,*б* показана полученная в результате квантования и кодирования последовательность двоичных видеоимпульсов. Из-за искажений сигналов и шумов в канале принятая видеопоследовательность (рис. 16,*в*) отличается от переданной. Выбирается

пороговый уровень S_0, его превышение в моменты отсчета (стробирования) значения сигнала означает наличие импульса, а непревышение – отсутствие импульса. С помощью формирующих устройств из принятой видеопоследовательности создается “очищенная” последовательность, которая поступает на декодер. С выхода декодера импульсы, площадь которых равна соответствующим импульсным отсчётам исходного сигнала (рис. 16,*д*), поступают на демодулятор, в простейшем случае на вход фильтра нижних частот, на выходе которого восстанавливается копия исходного непрерывного сигнала рис. 16,*д*.

Для получения регенерированной кодовой последовательности отсчёты принимаемого сигнала берутся в середине каждого тактового интервала

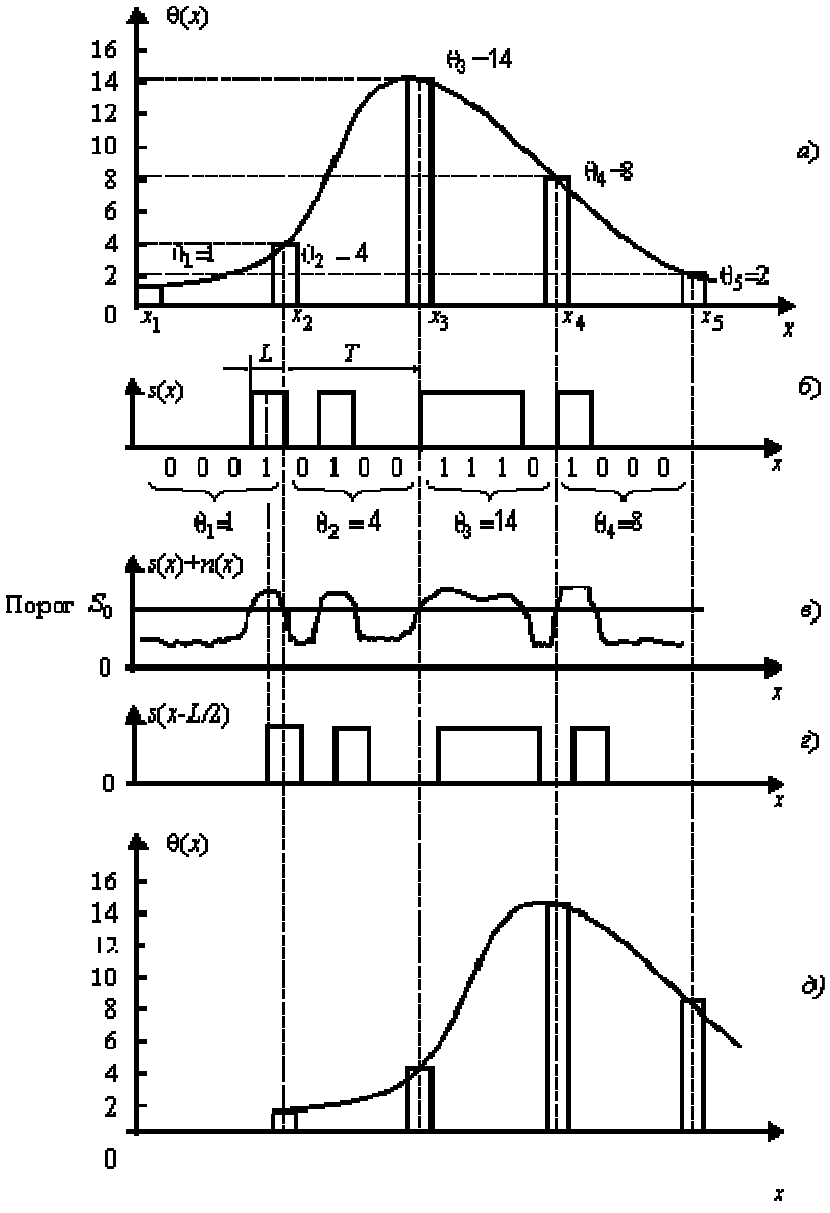


Рис. 16. Диаграммы сигналов в 4-разрядной системе ИКМ

длительностью L(рис. 16,*б* и *в*). Это делается для того, чтобы исключить влияние на работу демодулятора запаздывания и фазовых искажений сигналов в канале связи. В результате регенерируемая последовательность “задержана” на $L/2$ относительно

переданной (рис. 16,*б* и *г*). Правильное декодирование сигналов требует также, чтобы были приняты все разряды кодовой комбинации. Из-за этого принятые отсчёты оказываются дополнительно задержанными относительно передаваемых на интервал дискретизации *T* (рис. 16,а и д).

Метод пороговой селекции сигналов на фоне помех часто не обеспечивает требуемой помехоустойчивости и достоверности при приеме кодовых сигналов. Значительно более высокую помехоустойчивость обеспечивает применение метода согласованной фильтрации импульсных сигналов.

Проведем сравнительный анализ характеристик методов цифровой амплитудно-импульсной, импульсно-кодовой и фазоимпульсной модуляции при использовании согласованных фильтров.

Цифровая амплитудно-импульсная модуляция

Предположим, что кодовое сообщение представляет собой последовательность двоичных трехразрядных чисел в качестве одиночных слов. Таким образом, всего имеется $2^3 = 8$ возможных слов. В описываемых далее системах каждому из 8 слов ставится в соответствии отдельный сигнал длительностью в три тактовых импульса $3L$. В случае АИМ указанные восемь сигналов имеют форму импульсов с восемью возможными значениями амплитуды как показано на рис. 17. Максимальная амплитуда равна A, минимальная – 0, остальные значения амплитуды равномерно распределены как кратные величине $A/7$. Предположим, что указанный на рисунке сигнал $s(x)$ непосредственно передается по каналу. Спектр передаваемого АИМ сигнала имеет ширину $1/3L$, обратно пропорциональную длительности импульса. Если предположить, что восемь уровней равновероятны, то нетрудно доказать, что средняя мощность передаваемого АИМ сигнала равна $P_{ср} = 0{,}36A^2$.

Предполагается, что напряжение на входе приемника представляет собой передаваемый сигнал $s(x)$ с уменьшенной амплитудой (из-за ослабления в канале) и искаженный аддитивной помехой $n(x)$. Для простоты будем считать, что*n(x)* – белый шум с постоянной спектральной плотностью G_0 и что ослабление в канале отсутствует.

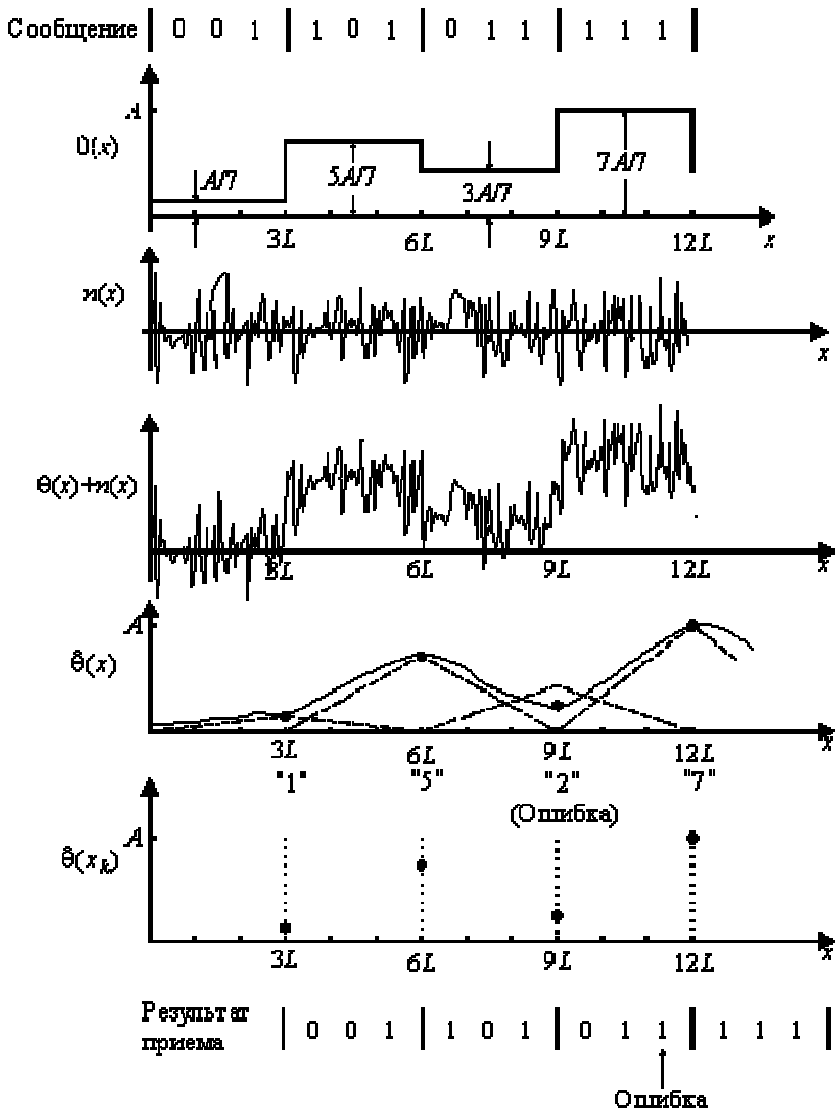


Рис. 17. Преобразование сигналов при цифровой АИМ

Чтобы восстановить кодовую последовательность, приемник усредняет принимаемый сигнал $\theta(x)+n(x)$ в течение каждого интервала $3L$. Это минимизирует влияние шума. Аналогичную операцию усреднения можно выполнить с помощью показанного на рис. 18 согласованного фильтра. Отклик согласованного фильтра $\hat{\theta}(x)$ на полезный сигнал $\theta(x)$ в принимаемом колебании представляет собой сумму треугольников, показанных пунктирными линиями на временной диаграмме рис. 17,*д*. Среднеквадратичное значение отклика согласованного фильтра на шумовую составляющую $n(x)$ равно

$$< n_ф^2(x) >= G_0 \int_{-\infty}^{\infty} h^2(x)dx = G_0 /3\,L \quad . (19)$$

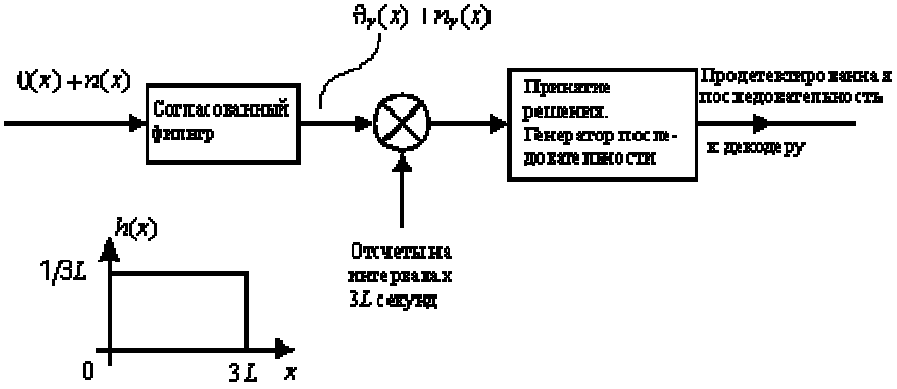


Рис. 18. Приемник АИМ сигнала с согласованным фильтром

Таким образом, величина каждой выборки на входе стробирующего устройства (рис. 18) состоит из суммы напряжения, равного амплитуде сигнала, т.е. $A/7$, $2A/7$, … , $7A/7$, и напряжения шума со среднеквадратичным значением $\sqrt{G_0/3L}$. Для того, чтобы принимаемое решение о том, какой уровень был передан на предыдущем интервале, имело высокую достоверность (низкую частоту ошибок), среднеквадратичное значение шума должно быть мало по сравнению с разностями между уровнями, т.е. для АИМ

$\sqrt{G_0/3L} << A/7$, (20)

или при условии $P_{cp} = 0{,}36A^2$ (средняя мощность передаваемого сигнала), $P_{cp}L/G_0 >> 5{,}88$. (21)

Это соотношение характеризует мощность передаваемого сигнала и скорость, с которой данная система может передавать двоичную информацию. Таким образом, видно, что полоса пропускания обменивается на отношение сигнал-шум. Этот важный принцип теории связи позволяет объяснить многие свойства методов модуляции, например, преимущество ЧМ над АМ.

Импульсно-кодовая модуляция

Различие между импульсно-кодовой модуляцией (ИКМ) и АИМ показано на рисунке 19. Каждый разряд двоичного числа передается в отдельности: 1 – импульсом длительностью *L*и амплитудой *B* , а 0 – отсутствием импульса. Если 0 и 1 равновероятны, то средняя мощность передаваемого сигнала равна $P_{cp} = 0{,}5B^2$, а его полоса составляет примерно $1/L$. Следовательно, ИКМ сигнал в рассматриваемом примере занимает в 3 раза более широкую полосу по сравнению с АИМ сигналом, что является серьезным недостатком.

Приемник системы ИКМ аналогичен приемнику для АИМ сигнала с тем отличием, что его согласованный фильтр должен иметь импульсную характеристику втрое меньшей длительности и в 3 раза более широкую полосу пропускания, как показано на рис. 20. В результате среднеквадратичное значение шумов на выходе приемника

$\langle n_y^2(x) \rangle = G_0 / L$ (22)

в 3 раза выше по сравнению со значением для АИМ приемника. Это является недостатком ИКМ сигнала. Однако разность между уровнями сигнала на входе устройства выборки ИКМ в приемнике равна максимальной амплитуде сигнала B, а не $1/7$ амплитуды, как в АИМ системе. Благодаря этому с запасом компенсируется повышенный уровень выходных шумов, поскольку для достижения малой вероятности ошибок в ИКМ системе требуется выполнить условие

$\sqrt{G_0 / L} << B$ (23)

или, полагая $0{,}5B^2 = P_{cp}$,

$P_{cp} L / G_0 >> 0{,}5$. (24)

При одной и той же вероятности ошибок ИКМ система может иметь примерно в 10 раз меньшую мощность сигнала по сравнению с АИМ. При равных мощностях ИКМ система имеет гораздо лучшие характеристики.

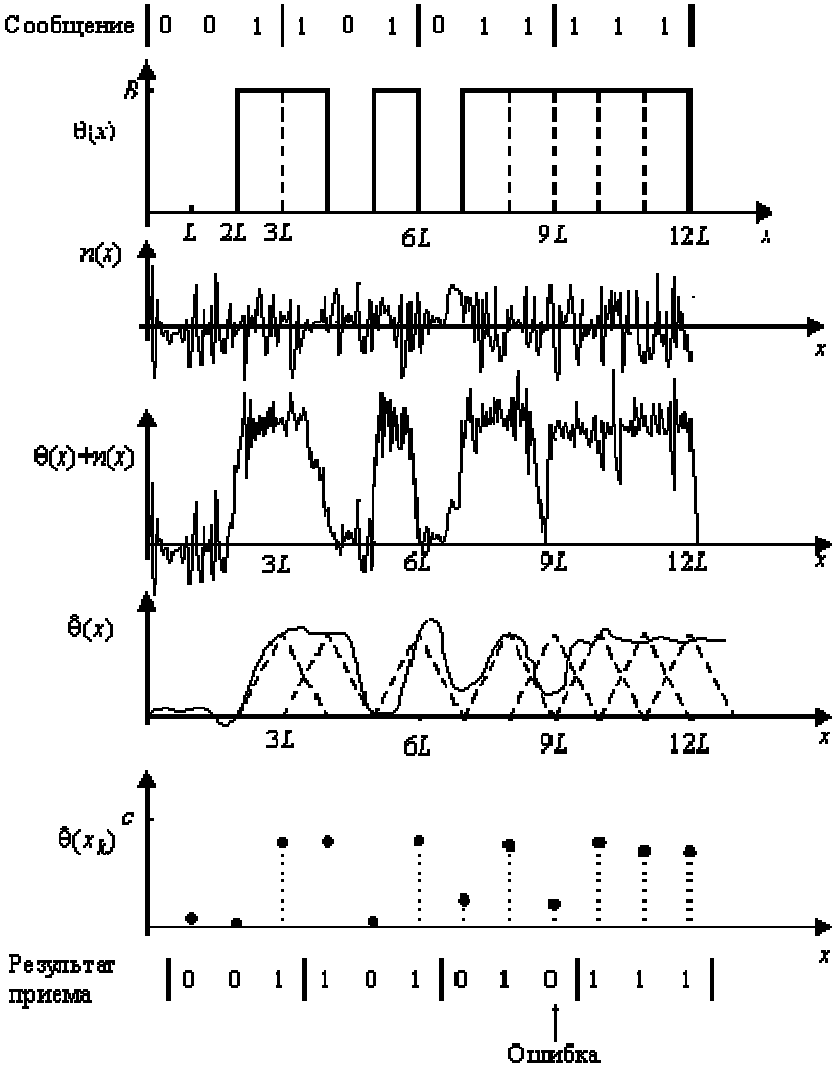


Рис. 19. Преобразование сигналов в ИКМ

Фазоимпульсная модуляция

Принцип фазоимпульсной модуляции иллюстрируется на рис. 21. По своим характеристикам она превосходит рассмотренную ИКМ систему, но этот выигрыш достигается за счет расширения полосы частот. В каждом интервале длительностью $3L$ передается один импульс с фиксированной амплитудой, но его длительность составляет всего $3L/8$ и он находится в одном из восьми временных положений. Таким образом, полоса указанного сигнала равна $8/3L$ или в 8 раз превышает полосу АИМ сигнала и в 2,7 раз больше полосы ИКМ сигнала. Средняя мощность сигнала составляет $P_{cp} = 0{,}125C^2$.

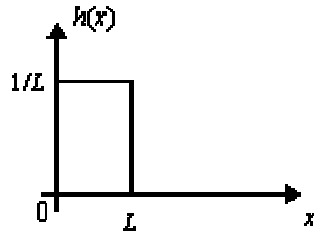


Рис. 20. Импульсный отклик согласованного фильтра протяженностью *L* для ИКМ сигнала; протяженностью 3*L/8* для ФИМ сигнала

Длительность импульсной характеристики согласованного фильтра составляет $3L/8$. Тогда среднеквадратическое значение выходного шума равно $\langle n_y^2(x) \rangle = 8G_0/3L$, что намного больше по сравнению с ИКМ или АИМ. Однако при этом значительно больше и разность между уровнями сигналов. Для достижения низкой вероятности ошибок необходимо обеспечить выполнение условия

$$\sqrt{8G_0/3L} << C \quad (25)$$

или, полагая $P_{cp} = 0{,}125C^2$,

$$P_{cp}L/G_0 > 0{,}33. \quad (26)$$

Следовательно, ФИМ система обеспечивает такое же качество, как и ИКМ при снижении на $1/3$ средней мощности сигнала, но требуемая полоса частот в этом случае расширяется в три раза. Таким образом, в смысле обмена полосы на соотношение сигнал-шум, ФИМ-система уступает ИКМ-системе.

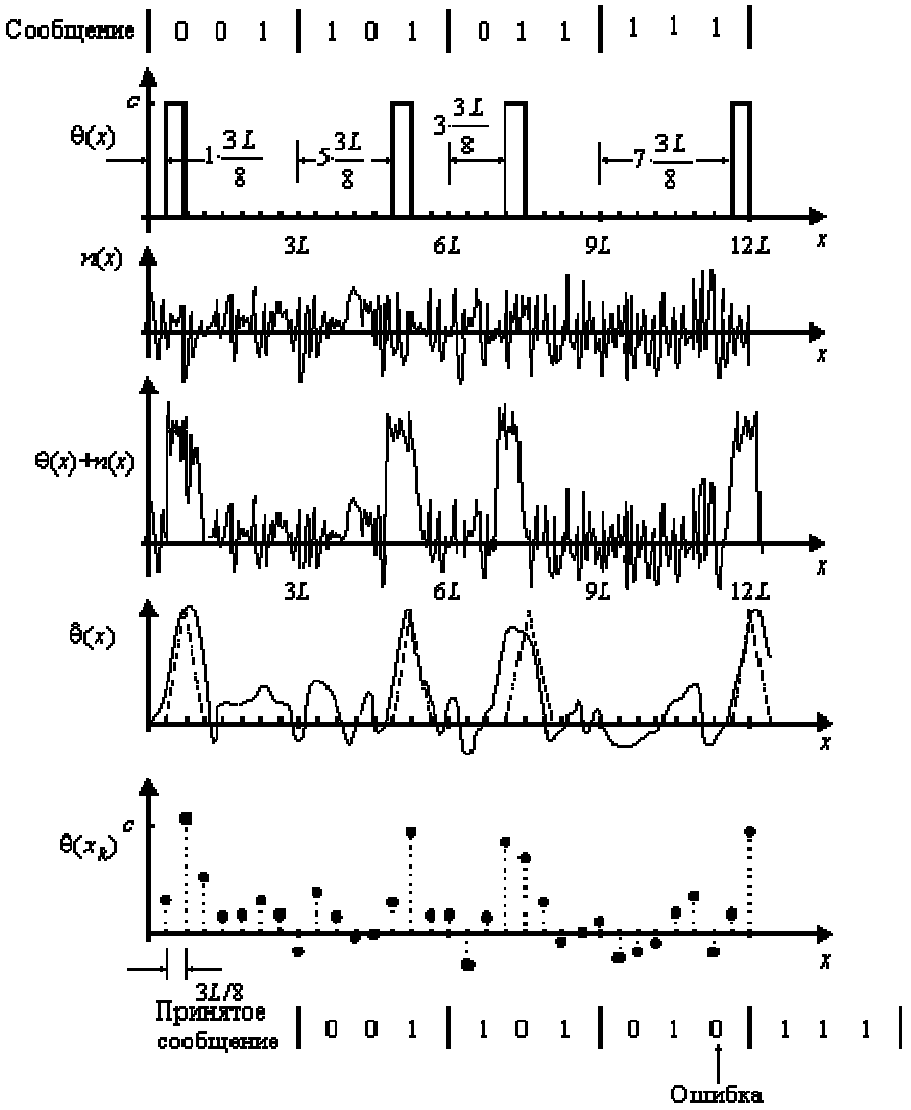


Рис. 21. Преобразование сигналов в ФИМ

Дельта-модуляция

Эффективным способом преобразования сигналов в цифровую форму является *дельта-модуляция*, которая иллюстрируется рис. 22. В каждый момент отсчета сигнал сравнивается с пилообразным напряжением на каждом шаге дискретизации d . Если отсчет сигнала превышает по амплитуде пилообразное напряжение, то последнее нарастает до следующей точки дискретизации, в противном случае оно спадает. В простейшей системе наклон пилообразного напряжения сохраняется неизменным на всем протяжении процесса. Полученный бинарный сигнал можно рассматривать как производную от пилообразного напряжения. Выбирая достаточно малым значение шага d , можно получить любую заданную точность представления сигнала. Преимущество дельта-модуляции по сравнению, например, с ИКМ, которая также образует бинарный сигнал, заключается не столько в реализуемой точности при заданной частоте дискретизации, сколько в простоте реализации.

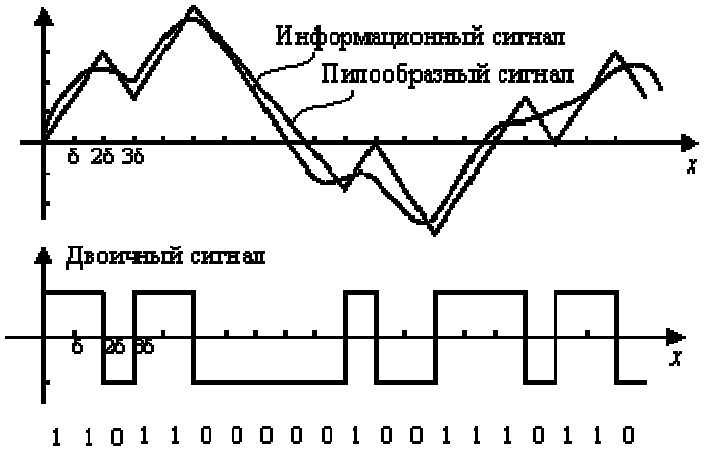


Рис. 22. Преобразование сигнала при дельта-модуляции

Пилообразное напряжение можно восстановить из бинарного сигнала путем интегрирования, а более гладкая аппроксимация достигается последующим пропусканием сигнала через фильтр нижних частот. Скорость передачи цифровых кодов, необходимую для получения заданного качества, можно значительно уменьшить, используя, например, линейное кодирование с предсказанием.

2.12 Лабораторная работа № 16, 17 (4 часа)

Тема: «Технология FDDI»

2.12.1 Цель работы: изучить базовые технологии локальных сетей FDDI.

2.12.2 Задачи работы:

1. Изучить технологию FDDI;
2. Ознакомиться с особенностями метода доступа FDDI.

2.12.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.12.4 Описание (ход) работы:

Технология FDDI

Технология *FDDI (Fiber Distributed Data Interface)*- оптоволоконный интерфейс распределенных данных - это первая технология локальных сетей, в которой средой передачи данных является волоконно-оптический кабель.

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

Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Наличие двух колец - это

основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят воспользоваться этим повышенным потенциалом надежности, должны быть подключены к обоим кольцам.

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

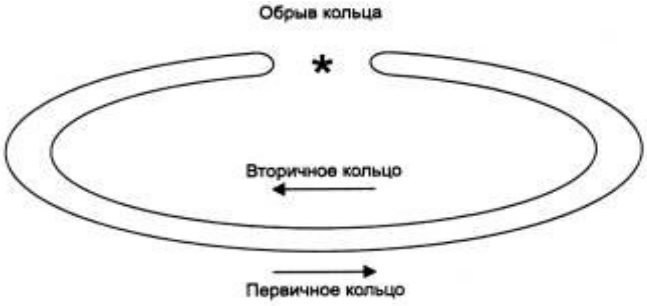


Рисунок 1 - Реконфигурация колец FDDI при отказе

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется со вторичным (рисунок 1), вновь образуя единое кольцо. Этот режим работы сети называется *Wrap,* то есть «свертывание» или «сворачивание» колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров FDDI. Для упрощения этой процедуры данные по первичному кольцу всегда передаются в одном направлении (на диаграммах это направление изображается против часовой стрелки), а по вторичному - в обратном (изображается по часовой стрелке). Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

Технология FDDI дополняет механизмы обнаружения отказов технологии Token Ring механизмами реконфигурации пути передачи данных в сети, основанными на наличии резервных связей, обеспечиваемых вторым кольцом.

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

Отличия метода доступа заключаются в том, что время удержания маркера в сети FDDI не является постоянной величиной, как в сети Token Ring. Это время зависит от загрузки кольца - при небольшой загрузке оно увеличивается, а при больших перегрузках

может уменьшаться до нуля. Эти изменения в методе доступа касаются только асинхронного трафика, который не критичен к небольшим задержкам передачи кадров. Для синхронного трафика время удержания маркера по-прежнему остается фиксированной величиной. Механизм приоритетов кадров, аналогичный принятому в технологии Token Ring, в технологии FDDI отсутствует. Разработчики технологии решили, что деление трафика на 8 уровней приоритетов избыточно и достаточно разделить трафик на два класса - асинхронный и синхронный, последний из которых обслуживается всегда, даже при перегрузках кольца.

В остальном пересылка кадров между станциями кольца на уровне MAC полностью соответствует технологии Token Ring. Станции FDDI применяют алгоритм раннего освобождения маркера, как и сети Token Ring со скоростью 16 Мбит/с.

Скорость передачи данных для сетей FDDI составляет 100 Мбит/с. Максимальное число узлов составляет 500. При использовании в качестве физической среды передачи данных многомодового оптоволоконного кабеля расстояние между узлами сети может доходить до 2 км, а при использовании одномодового кабеля – до 40 км. В случае кабеля на основе витых пар пятой категории это расстояние не превышает 100 м. максимальный диаметр двойного кольца не должен превышать 100 км.

Адреса уровня MAC имеют стандартный для технологий IEEE 802 формат. Формат кадра FDDI близок к формату кадра Token Ring, основные отличия заключаются в отсутствии полей приоритетов.

Особенности метода доступа FDDI.

Для передачи синхронных кадров станция всегда имеет право захватить маркер при его поступлении. При этом время удержания маркера имеет заранее заданную фиксированную величину.

Если же станции кольца FDDI нужно передать асинхронный кадр (тип кадра определяется протоколами верхних уровней), то для выяснения возможности захвата маркера при его очередном поступлении станция должна измерить интервал времени, который прошел с момента предыдущего прихода маркера. Этот интервал называется временем оборота маркера. Если в технологии Token Ring максимально допустимое время оборота маркера является фиксированной величиной (2,6 сиз расчета 260 станций в кольце), то в технологии FDDI станции договариваются о его величине во время инициализации кольца. Каждая станция может предложить свое значение, в результате для кольца устанавливается минимальное из предложенных станциями времен. Это позволяет учитывать потребности приложений, работающих на станциях. Обычно синхронным приложениям (приложениям реального времени) нужно чаще передавать данные в сеть небольшими

порциями, а асинхронным приложениям лучше получать доступ к сети реже, но большими порциями. Предпочтение отдается станциям, передающим синхронный трафик.

Для обеспечения отказоустойчивости в стандарте FDDI предусмотрено создание двух оптоволоконных колец - первичного и вторичного. В стандарте FDDI допускаются два вида подсоединения станций к сети. Одновременное подключение к первичному и вторичному кольцам называется двойным подключением - Dual Attachment, DA. Подключение только к первичному кольцу называется одиночным подключением - Single Attachment, SA.

В стандарте FDDI предусмотрено наличие в сети конечных узлов – станций и также концентраторов. Для станций и концентраторов допустим любой вид подключения к сети - как одиночный, так и двойной. Обычно концентраторы имеют двойное подключение, а станции - одинарное, как это показано на рисунке 2, хотя это и не обязательно. Чтобы устройства легче было правильно присоединять к сети, их разъемы маркируются. Разъемы типа A и B должны быть у устройств с двойным подключением, разъем M (Master) имеется у концентратора для одиночного подключения станции, у которой ответный разъем должен иметь тип S (Slave).

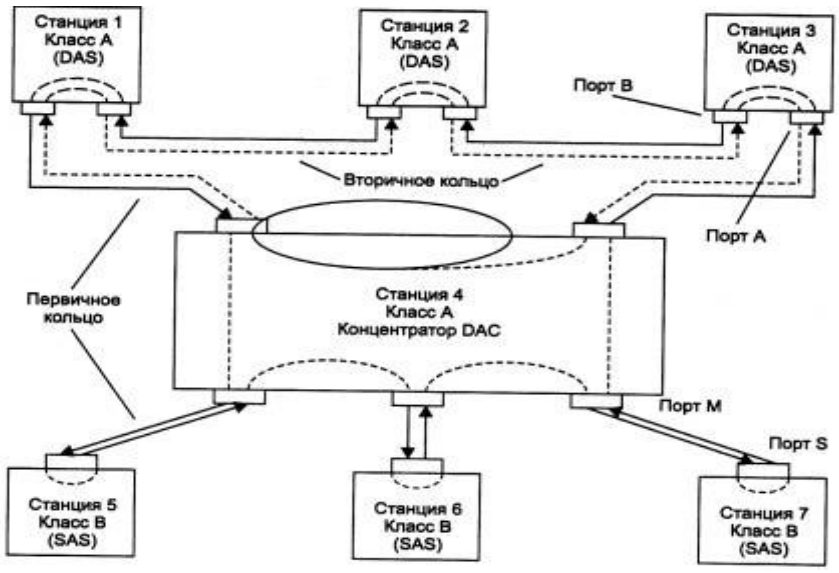


Рисунок 2 – Подключение узлов к кольцам FDDI. SAS (Single Attachment Station), DAS (Dual Attachment Station), SAC (Single Attachment Concentrator) и DAC (Dual Attachment Concentrator).

Стандарт **FDDI** (*Fiber Distributed Data Interface*□ волоконно-оптический интерфейс передачи данных), разработанный в середине 80-х годов комитетом X3T9.5 ANSI, определяет кольцевую сеть с маркерным доступом и скоростью передачи до 100 Мбит/с на основе волоконно-оптического кабеля, способною охватить очень большую площадь (до 100 км).

Стандарт FDDI во многом основывается на технологии Token Ring (стандарт IEEE 802.5) и обеспечивает совместимость с ней, т.к. у обеих технологий одинаковые форматы кадров. Однако у этих технологий имеются существенные различия.

Стек FDDI определяет физический уровень и подуровень доступа к среде передачи

(MAC). Физический уровень разбит на протокол физического уровня (Physical Layer Protocol, PHY), который отвечает за работу схем кодирования данных, и на подуровень физического уровня, зависящий от среды передачи (Physical Medium Dependent, PMD), на котором реализованы спецификации передачи. Особенностью стека FDDI является наличие уровня управления станциями (Station Management, SMT). Он отвечает за удаление и подключение рабочих станций, обнаружение и устранение неисправностей, сбор статистической информации о работе сети.

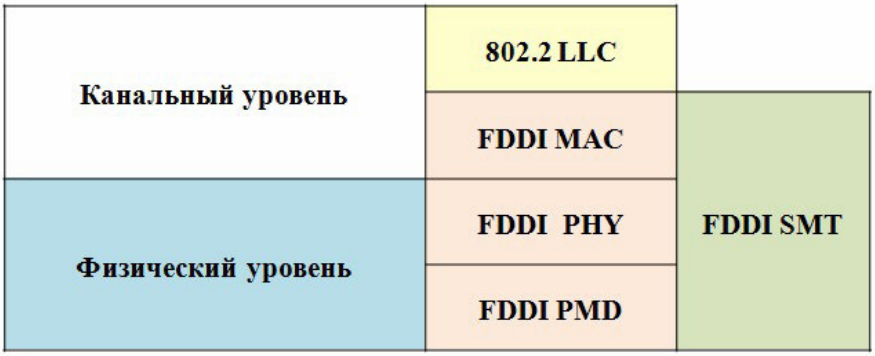


Рисунок 3.Стек FDDI

Сети FDDI характеризуются встроенной избыточностью, что обеспечивает их высокую отказоустойчивость. Сеть FDDI строится на основе двух колец, которые образуют основной и резервный пути передачи данных между узлами сети. Данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным (первичным). По нему данные передаются при нормальной работе. Второе кольцо (вторичное) вспомогательное, по нему данные передаются в случае обрыва в первом кольце. В случае какого-либо вида отказа, когда часть первого кольца не может передавать данные (например, обрыв кабеля или отказ узла), сеть выполняет «свертывание» колец объединяет первое кольцо со вторым, образуя единое кольцо.

Основными компонентами сети FDDI являются станции и концентраторы. Для подключения станций и концентраторов к сети может быть использован один из двух способов:

- **Одиночное подключение** (Single Attachment, SA) подключение только к первичному кольцу. Станция и концентратор, подключенные данным способом, называются соответственно станцией одиночного подключения (Single Attachment

Station, SAS) и концентратором одиночного подключения (Single Attachment Concentrator, SAC).

- **Двойное подключение** (Dual Attachment, DA) одновременное подключение к первичному и вторичному кольцам. Станция и концентратор, подключенные таким способом, называются соответственно станцией двойного подключения (Dual Attachment Station, DAS) и концентратором двойного подключения (Dual Attachment Concentrator, DAC).

В качестве среды передачи в сетях FDDI используется одномодовый и многомодовый волоконно-оптический кабель. Максимальное количество станций в кольце – 500. Максимальное расстояние между узлами может составлять 2 км при использовании многомодового кабеля и 20 км – при использовании одномодового. Максимальная протяженность сети – 100 км.

К преимуществам технологии FDDI можно отнести высокую отказоустойчивость. К недостаткам – двойной расход кабеля.

В настоящее время эта технология считается устаревшей.

Контрольные вопросы

1) Что означает аббревиатура FDDI?
2) Объясните метод доступа в сетях FDDI.
3) Как повышается отказоустойчивость в сетях FDDI?
4) Сравните технологии FDDI и Token Ring (в таблице).

2.13 Лабораторная работа № 18, 19 (4 часа)

Тема: «Технология ATM»

2.13.1 Цель работы: изучить базовые технологии локальных сетей ATM.

2.13.2 Задачи работы:

1. Изучить технологию ATMI;
2. Ознакомиться с особенностями ATM.

2.13.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.13.4 Описание (ход) работы:

Корпоративные сетевые стандарты позволяют обеспечить эффективное взаимодействие всех станций сети за счет использования одинаковых версий программ и однотипной конфигурации. Однако, значительные сложности возникают при унификации технологии доступа рабочих станций к WAN-сервису, поскольку в этом случае происходит преобразование данных из формата token ring или Ethernet в форматы типа X.25 или T1/E1.

ATM обеспечивает связь между станциями одной сети или передачу данных через WAN-сети без изменения формата ячеек - технология ATM является универсальным решением для ЛВС и телекоммуникаций.

Нет сомнений в том, что скоростные технологии ЛВС являются основой современных сетей. ATM, FDDI и Fast Ethernet являются основными вариантами дляорганизация сетей с учетом перспективы. Очевидно, что приложениям multimedia, системам обработки изображений, CAD/CAM, Internet и др. требуется широкополосный доступ в сеть с рабочих станций. Все современные технологии обеспечивают высокую скорость доступа для рабочих станций, но только ATM обеспечивает эффективную связь между локальными и WAN-сетями.

ATM - история и базовые принципы

Технология ATM сначала рассматривалась исключительно как способ снижения телекоммуникационных расходов, возможность использования в ЛВС просто не принималась во внимание. Большинство широкополосных приложений отличается взрывным характером трафика. Высокопроизводительные приложения типа ЛВС клиент-сервер требуют высокой скорости передачи в активном состоянии и практически не используют сеть в остальное время. При этом система находится в активном состоянии (обмен данными) достаточно малое время. Даже в тех случаях, когда пользователям реально не нужна обеспечиваемая сетью полоса, традиционные технологии ЛВС все равно ее выделяют. Следовательно, пользователям приходится платить за излишнюю полосу. Перевод распределенных сетей на технологию ATM позволяет избавиться от таких ненужных расходов.

Комитеты по стандартизации рассматривали решения для обеспечения недорогих широкополосных систем связи в начале 80-х годов. Важно то, что целью этого рассмотрения было применение принципов коммутации пакетов или статистического мультиплексирования, которые так эффективно обеспечивают передачу данных, к системам передачи других типов трафика. Вместо выделения специальных сетевых ресурсов для каждого соединения сети с коммутацией пакетов выделяют ресурсы по запросам (сеансовые соединения). Поскольку для каждого соединения ресурсы выделяются только на время их реального использования, не возникает больших проблем из-за спада трафика.

Проблема, однако, состоит в том, что статистическое мультиплексирование не обеспечивает гарантированного выделения полосы для приложений. Если множество пользователей одновременно захотят использовать сетевые ресурсы, кому-то может просто не хватить полосы. Таким образом, статистическое мультиплексирование, весьма эффективное для передачи данных (где не требуется обеспечивать гарантированную

незначительную задержку), оказывается малопригодным для систем реального времени (передача голоса или видео). Технология ATM позволяет решить эту проблему.

Проблема задержек при статистическом мультиплексировании связана в частности с большим и непостоянным размером передаваемых по сети пакетов информации. Возможна задержка небольших пакетов важной информации из-за передачи больших пакетов малозначимых данных. Если небольшой задержанный пакет оказывается частью слова из телефонного разговора или multimedia-презентации, эффект задержки может оказаться весьма существенным и заметным для пользователя. По этой причине многие специалисты считают, что статистическое мультиплексирование кадров данных дает слишком сильную дрожь из-за вариации задержки (delay jitter) и не позволяет предсказать время доставки. С этой точки зрения технология коммутации пакетов является совершенно неприемлемой для передачи трафика типа голоса или видео.

ATM решает эту проблему за счет деления информации любого типа на небольшие ячейки фиксированной длины. Ячейка ATM имеет размер 53 байта, пять из которых составляют заголовок, оставшиеся 48 - собственно информацию. В сетях ATM данные должны вводиться в форме ячеек или преобразовываться в ячейки с помощью функций адаптации. Сети ATM состоят из коммутаторов, соединенных транковыми каналами ATM. Краевые коммутаторы, к которым подключаются пользовательские устройства, обеспечивают функции адаптации, если ATM не используется вплоть до пользовательских станций. Другие коммутаторы, расположенные в центре сети, обеспечивают перенос ячеек, разделение транков и распределение потоков данных. В точке приема функции адаптации восстанавливают из ячеек исходный поток данных и передают его устройству-получателю, как показано на рисунке 4.1.

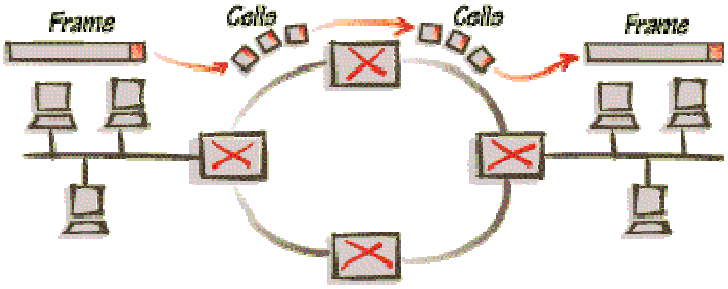


Рисунок 1 Адаптация ATM

Передача данных в коротких ячейках позволяет ATM эффективно управлять потоками различной информации и обеспечивает возможность приоритизации трафика.

Пусть два устройства передают в сеть ATM данные, срочность доставки которых различается (например, голос и трафик ЛВС). Сначала каждый из отправителей делит передаваемые данные на ячейки. Даже после того, как данные от одного из отправителей

будут приниматься в сеть, они могут чередоваться с более срочной информацией. Чередование может осуществляться на уровне целых ячеек и малые размеры последних обеспечивают в любом случае непродолжительную задержку.такое решение позволяет передавать срочный трафик практически без задержек, приостанавливая на это время передачу некритичной к задержкам информации. В результате АТМ может обеспечивать эффективную передачу всех типов трафика.

Даже при чередовании и приоритизации ячеек в сетях АТМ могут наступать ситуации насыщения пропускной способности. Для сохранения минимальной задержки даже в таких случаях АТМ может отбрасывать отдельные ячейки при насыщении. Реализация стратегии отбрасывания ячеек зависит от производителя оборудования АТМ, но в общем случае обычно отбрасываются ячейки с низким приоритетом (например, данные) для которых достаточно просто повторить передачу без потери информации. Коммутаторы АТМ с расширенными функциями могут при отбрасывании ячеек, являющихся частью большого пакета, обеспечить отбрасывание и оставшихся ячеек из этого пакета - такой подход позволяет дополнительно снизить уровень насыщения и избавиться от излишнего объема повторной передачи. Правила отбрасывания ячеек, задержки данных и т.п. определяются набором параметров, называемым качеством обслуживания (Quality of Service) или QoS. Разным приложениям требуется различный уровень QoS и АТМ может обеспечить этот уровень.

Поскольку приходящие из разных источников ячейки могут содержать голос, данные и видео, требуется обеспечить независимый контроль для передачи всех типов трафика. Для решения этой задачи используется концепция виртуальных устройств. Виртуальным устройством называется связанный набор сетевых ресурсов, который выглядит как реальное соединение между пользователями, но на самом деле является частью разделяемого множеством пользователей оборудования. Для того, чтобы сделать связь пользователей с сетями АТМ как можно более эффективной, виртуальные устройства включают пользовательское оборудование, средства доступа в сеть и собственно сеть АТМ.

В заголовке АТМ виртуальный канал обозначается комбинацией двух полей - VPI (идентификатор виртуального пути) и VCI (идентификатор виртуального канала. Виртуальный путь применяется в тех случаях, когда 2 пользователя АТМ имеют свои собственные коммутаторы на каждом конце пути и могут, следовательно, организовывать и поддерживать свои виртуальные соединения. Виртуальный путь напоминает канал, содержащий множество кабелей, по каждому из которых может быть организовано виртуальное соединение.

Поскольку виртуальные устройства подобны реальным, они также могут быть "выделенными" или "коммутируемыми". В сетях АТМ "выделенные" соединения

называются постоянными виртуальными устройствами (PVC), создаваемыми по соглашению между пользователем и оператором (подобно выделенной телефонной линии). Коммутируемые соединения ATM используют коммутируемые виртуальные устройства (SVC), которые устанавливаются путем передачи специальных сигналов между пользователем и сетью. Протокол, используемый ATM для управления виртуальными устройствами подобен протоколу ISDN. Вариант для ISDN описан в стандарте Q.931, ATM - в Q.2931.

Виртуальные устройства ATM поддерживаются за счет мультиплексирования трафика, что существенно снижает расходы на организацию и поддержку магистральных сетей.если в одном из виртуальных устройств уровень трафика невысок, другое устройство может использовать часть свободных возможностей. За счет этого обеспечивается высокий уровень эффективности использования пропускной способности ATM и снижаются цены. Небольшие ячейки фиксированной длины позволяют сетям ATM обеспечить быструю передачу критичного к задержкам трафика (например, голосового). Кроме того, фиксированный размер ячеек обеспечивает практически постоянную задержку, позволяя эмулировать устройства с фиксированной скоростью передачи типа T1E1. Фактически, ATM может эмулировать все существующие сегодня типы сервиса и обеспечивать новые услуги. ATM обеспечивает несколько классов обслуживания, каждый из которых имеет свою спецификацию QoS.

Класс QoS	**Класс обслуживания**	**Описание**
1	A	производительность частных цифровых линий (эмуляция устройств или CBR)
2	B	пакетные аудио/видео-конференции и multimedia (rt-VBR)
3	C	ориентированные на соединения протоколы типа frame relay (nrt-VBR)
4	D	протоколы без организации соединений типа IP, эмуляция ЛВС (ABR)
5	Unspecified	наилучшие возможности в соответствии с определением оператора (UBR)

Большая часть трафика, передаваемого через сети ATM использует класс обслуживания C, X или Y. Класс C определяет параметры QoS (качество обслуживания) для задержки и вероятности отбрасывания, но требует от пользователя аккуратного управления трафиком во избежание перенасыщения сети.трафик класса X дает пользователю большую

свободу, но может не обеспечить стабильной производительности. Класс Y, называемый также "Available Bit Rate" (ABR или доступная скорость) позволяет пользователю и сети установить совместно скорость на основе оценки потребностей пользователя и возможностей сети.

ATM как технология ЛВС

Технология ATM изначально создавалась как часть сервиса "Broadband ISDN" под эгидой CCITT (сейчас ITU). Однако возможности ATM можно эффективно использовать и в локальных сетях.

Современные крупные сети используются для передачи самых разных типов данных, включая изображения, звук, CAD/CAM и т.п. Несмотря на то, что большинство компьютерных приложений используется уже достаточно давно, возможности современных настольных компьютеров позволяют по новому подойти к организации работы. Однако, рост возможностей настольных компьютеров существенно опережает расширение сетевых возможностей (в частности, пропускной способности сетей).

Возьмем для примера издательские системы, где с одним набором данных может одновременно работать множество людей. Представьте себе процесс подготовки газетной полосы для публикации.редакторы работают с одной частью полосы, корректоры просматривают текст, дизайнеры размещают материал на полосе - и все это происходит в одно время. Не будем забывать и о том, что высокое качество печати требует использования графических фалов размером в сотни мегабайт. Традиционные сети обеспечивают разделение доступа к таким файлам, однако из-за ограниченной пропускной способности доступ к расположенному на другом компьютере файлу размером в несколько сот мегабайт будет отнюдь не быстрым. ATM 25 позволяет пользователям организовать каналы доступа с полосой 25 Мбит/с для работы с серверами. Такое решение избавляет от задержек и позволяет готовить публикации существенно быстрее.

Преимущества ATM не ограничиваются вертикальным рынком. Сегодня организации могут связать через магистрали ATM свои корпоративные серверы. Можно ожидать и достаточно широкого использования ATM в настольных компьютерах при работе пользователей с большими объемами данных или использовании критичных к задержкам приложений.

Экономический фактор играет далеко не последнюю роль в расширении использования технологий ATM. Сегодня большинство людей использует в своей работе и телефон и компьютер. В течение нескольких лет существенно расширится обмен данными multimedia (клипами), использование видеоконференций и т.п. технология ISDN позволяет решить такие задачи. Однако, это потребует установки оборудования ISDN в каждый компьютер. Телефонные и сетевые кабельные системы не могут полностью совпадать, что

дополнительно увеличивает сложность такого решения. Использование решения на базе ISDN с необходимостью приведет к возникновению параллельных кабельных систем для ЛВС и телефонии и подключению каждого компьютера к обеим системам. Нужно учесть еще и телевизионные кабели, которые также требуется проложить по причине расширения использования настольных видео-приложений. Такая кабельная система будет весьма сложна, а ее установка и поддержка потребуют высоких расходов. Переход на использование технологии ATM в локальных сетях позволяет обойтись одной кабельной системой и одним адаптером в компьютере, что не может не привести к значительному снижению расходов.

ATM позволяет не только организовать ЛВС, но может обеспечить передачу голосового и видео-трафика. Такое решение позволяет использовать настольные системы видеоконференций и приложения multimedia.

Фактически, использование ATM обеспечивает сразу множество преимуществ. Во-первых, высокая скорость доступа за приемлемую цену, во-вторых, возможность организации компактных магистралей на базе ATM (collapsed backbone). Наконец, эта архитектура обеспечивает сквозное повышение эффективности использования сетевых ресурсов.

Пользователи, которые думают об использовании ATM в будущем, должны использовать совместимые с ATM устройства уже сегодня - в противном случае переход может оказаться слишком дорогим и трудоемким. Мы рассмотрим этот вопрос более подробно в следующем разделе.

ATM как современная инфраструктура

Если виртуальные устройства напоминают реальные, ATM можно легко приспособить для текущих приложений, просто заменив выделенные или коммутируемые линии виртуальными устройствами ATM. Фактически, этот способ вместе с переходом на ATM в сетевых магистралях, является наиболее очевидным первым шагом.

На рисунках 4.2, 4.3 и 4.4 показан типичный пользовательский сайт с устройствами, порождающими разнотипный трафик (голос, видео, данные). Эти три типа трафика могут передаваться с использованием сервиса ATM тремя показанными на рисунках способами.

1. Голос, данные и видео преобразуются в ячейки ATM в сети оператора с использованием функций адаптации ATM. Оператор будет реализовать все функции доступа и передачи, а для каждого устройства потребуется отдельная линия доступа в сеть ATM.

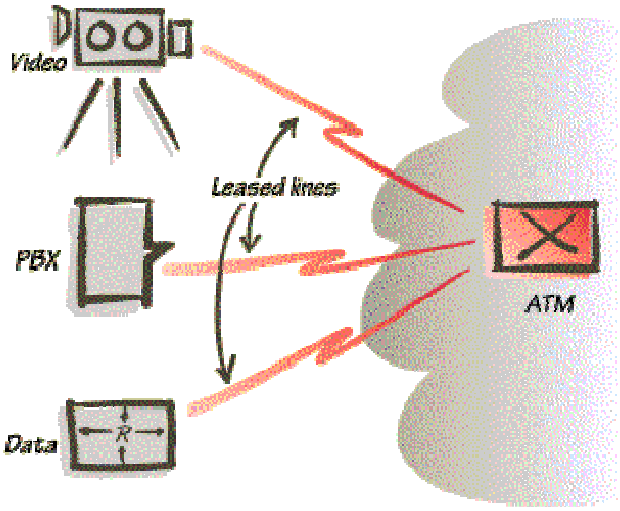


Рисунок 2 Преобразование в ATM осуществляется оператором

2. ЛВС, голосовые и видео-устройства подключаются к локальному коммутатору ATM для преобразования трафика в ячейки. Для доступа в сеть оператора используется одна линия, передающая все потоки трафика одновременно (как виртуальные устройства). Сеть оператора обеспечивает маршрутизацию трафика. Такое решение более экономично и может использоваться для организации "частных сетей ATM" для пользователей, которые имеют доступ к ATM-сервису или хотят создать свою распределенную сеть на базе ATM. Отметим, что находящийся в сети пользователя коммутатор ATM может принадлежать оператору и находиться у него на обслуживании.

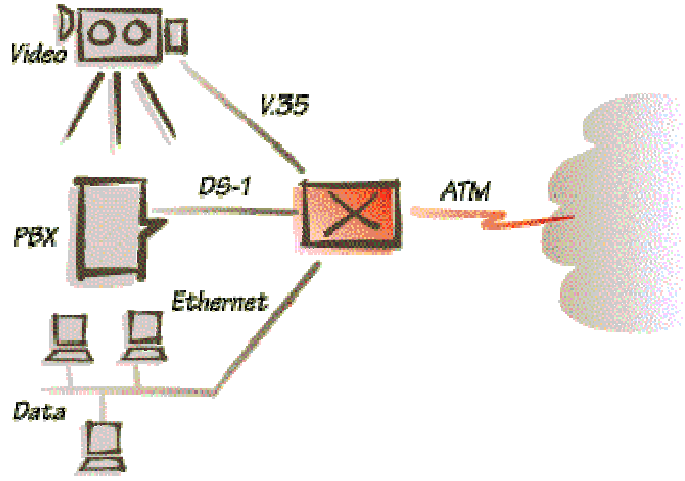


Рисунок 3 Преобразование в ATM осуществляется у пользователя

3. Устройства оборудуются собственными интерфейсами ATM. Одно устройство доступа позволяет объединить весь пользовательский трафик в одном транке, связанном с сетью оператора. В этом случае на стороне пользователя устанавливается принадлежащее ему оборудование ATM, которое можно использовать для организации магистралей ЛВС или подключения настольных станций.

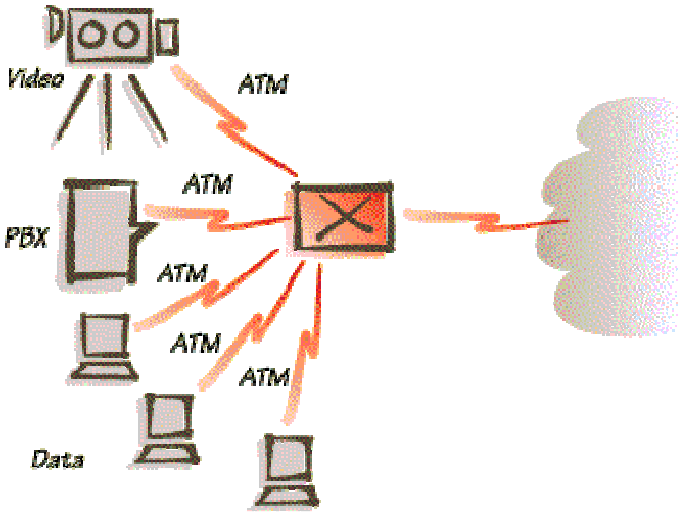


Рисунок 4 Сеть на базе ATM

Скорое появление интерфейсов ATM в телефонном и видеооборудовании не представляется вероятным, поэтому реализация третьего варианта соединения с сетью не сможет в ближайшие годы стать доминирующей. Фактически, скорость распространения каждого из приведенных вариантов будет определяться темпами снижения цен на оборудование и услуги операторов сетей ATM. Отсутствие эффективного управления этими процессами порождает определенный хаос и не позволяет надежно предсказать перспективы того или иного сервиса ATM.

Стандарт, определяющий интерфейс между операторами и пользователями ATM называется Public User Network Interface или Public UNI. Этот интерфейс определяется для различных значений скорости. Первые услуги ATM предлагались в основном со скоростью T3 (45 Мбит/с). Сейчас многие операторы предлагают скорость 155 Мбит/с и выше, но такая полоса обычно не требуется пользователям, да и стоимость подобных услуг весьма высока. Для большинства пользователей, планирующих организовать доступ к ATM или создать частную сеть ATM основной проблемой является стоимость оборудования.

Форум ATM - организация производителей оборудования ATM и пользователей работает в направлении развития стандартов и обеспечения интероперабельности оборудования. В конечном итоге это не может не привести к снижению цен. Кроме обеспечения интероперабельности ATM ведется большая работа по реализации ATM на скоростях меньше T3. Здесь возможно несколько вариантов:

1. Полнофункциональные решения ATM при скорости T1. Один стандарт для ATM T1 уже утвержден, но некоторые производители и пользователи считают, что связанные с реализацией этого стандарта накладные расходы слишком велики - канал T1 с полосой 1.544 Мбит/с может обеспечить полезную полосу только около 1.1 Мбит/с.

2. Так называемый dixie-стандарт (от акронима DXI - Data eXchange Interface). DXI был разработан как способ использования ATM в кадровом режиме с маршрутизаторами и другими устройствами передачи данных и специальными устройствами DSU, обеспечивающими преобразование кадров в реальные ячейки ATM. DXI работает через стандартные интерфейсы типа V.35 и HSSI.

3. Интерфейс пользователь - сеть Frame Relay или F-UNI (произностися как FOONY), являющийся стандартом использования frame relay для доставки "кадров данных ATM" в сеть, которая будет конвертировать их в ячейки непосредственно на границе сети.

4. Инверсное мультиплексирование ATM или AIM - стандарт для инверсного мультиплексирования множества линий T1 в один транк с полосой между T1 и T3. Такая полоса обеспечивает поддержку ATM для приложений, где скоростные запросы незначительно превышают возможности T1.

Проверка этих вариантов показывает, что они в основном подходят для систем обмена данными. Причиной этого является эффективная поддержка технологией ATM взрывного трафика современных систем передачи данных (ЛВС). Как было отмечено выше ATM может просто использоваться взамен выделенных линий в таких сетях, обеспечивая коммутацию ЛВС, поддерживаемую ATM UNI.

Замена выделенных линий системами ATM позволяет более эффективно организовать сети. Отметим, что виртуальные устройства ATM используются для организации многосвязных систем, позволяющих обеспечить доставку трафика непосредственно адресату. Сегодня желание пользователей применять многосвязные системы на базе ATM для связи своих сетей в значительной мере определяется предлагаемыми операторами ценами на услуги. Если оператор берет деньги за каждое виртуальное устройство ATM UNI, а не за общий трафик, стоимость организации многосвязной сети может оказаться слишком велика. Конечно, в кампусной магистрали ATM стоимость полосы в многосвязной системе будет несравненно ниже. Поддержка многосвязности требует лишь прокладки дополнительных физических соединений (кабелей) и установки более скоростных транковых портов в коммутаторы. Эти дополнительные расходы достаточно малы по сравнению с общей стоимостью сети.

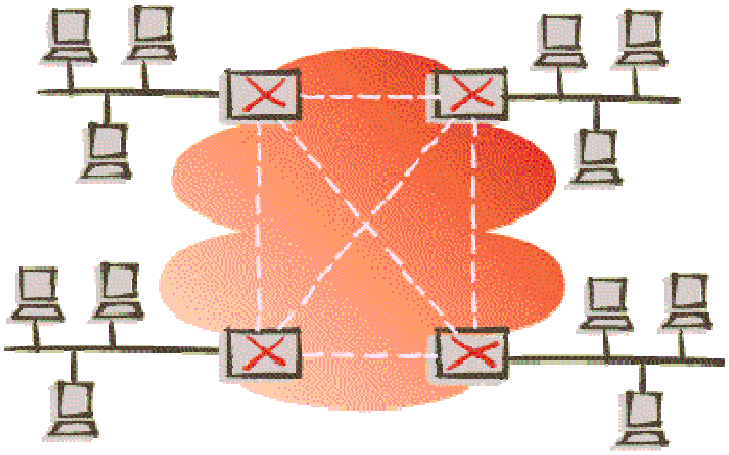


Рисунок 5 Многосвязная сеть

В многосвязной (каждый с каждым) сети ATM существует меньше транзитных точек, снижающих производительность и вносящих дополнительные задержки и насыщение. Такое решение обеспечивает существенное повышение стабильности работы приложений. Более того, каждый коммутатор является соседом для всех остальных коммутаторов и связан с ними напрямую. Это упрощает задачу динамического определения маршрута для протоколов маршрутизации типа RIP, используемого TCP/IP или NetWare, OSPF или IS-IS. Эти протоколы часто генерируют значительный трафик и могут существенно замедлить сеть при обмене конфигурационными данными (интервал сближения или конвергенции).

Если существует способ передачи "телефонного номера" ATM точке публичной сети ATM, которая достаточно близка к пользователям традиционной ЛВС, насколько можно приблизиться к пользователям? Ближайшей, готовой к использованию ATM станцией, сегодня является коммутатор. Это может быть магистральный коммутатор пользователя, коммутатор рабочей группы или даже настольный компьютер с адаптером ATM. В этом случае ATM используется как универсальная архитектура для коммуникаций, обеспечивающая связь между настольными системами вместе с традиционными технологиями ЛВС, а в некоторых случаях - взамен их. Это наиболее интересная, но и наиболее спорная часть применений ATM.

Сквозная ATM-парадигма для сетей

ATM на настольных станциях имеет несколько преимуществ. Во-первых, способность ATM гарантировать для приложений качество обслуживания (QoS) обеспечивает сквозную передачу критичного к задержкам трафика типа видео или голоса. Будучи технологией передачи данных, ATM не только может поддерживать "приложения завтрашнего дня", но и эффективно справляется с сегодняшними задачами. Пользователи задаются двумя основными вопросами - как будут формироваться распределенные сети на базе ATM и какие шаги нужно предпринять, чтобы быть готовым к переходу? Есть три разных варианта

включения ATM в архитектуру межсетевого взаимодействия для современных и будущих приложений:

1. Эмуляция традиционных протоколов ЛВС с использованием оборудования ATM. В этом случае существующие приложения будут продолжать работать как раньше, а ATM-добавит к существующим протоколам новые, специально разработанные для приложений multimedia. Отметим, что слово "новые" в данном контексте отнюдь не означает, что эти протоколы еще не существуют (они скорее еще не стали общепринятыми).

2. Подключение сервиса ATM напрямую к интерфейсам прикладных программ, используемых сегодня, в обход традиционных протоколов нижних уровней. Для поддержки этого варианта потребуется разработка новых API.

3. Использование новых API для "новых" приложений и эмуляция традиционных протоколов для существующих приложений.

Поскольку использование ATM обычно начинается с нескольких станций, которым требуются multimedia-приложения, требуется обеспечить эмуляцию традиционных протоколов ЛВС в сетях ATM. Это позволяет обеспечить надежное взаимодействие между новыми станциями на базе ATM и традиционными ЛВС. Для эмуляции ЛВС в системах на базе ATM (ATM LAN emulation) предложены два варианта - ATM Forum LAN Emulation (LANE) и RFC 1577. Говоря здесь об эмуляции, мы имеем в виду оба варианта.

Как LANE, так и RFC 1577 основаны на допущении что пользователи ATM применяют адаптеры, поддерживающие интерфейс ATM UNI. Поскольку этот интерфейс располагается со стороны пользователя, его иногда называют "Private UNI"; существует набор стандартов, определяющих данный интерфейс. Стандарты Private UNI существуют для скоростей 25 Мбит/с (по медному кабелю), 100 Мбит/с (оптический кабель)и 155 Мбит/с (медь и оптика). Оба стандарта эмуляции ЛВС предполагают также, что пользователи подключены к коммутатору ATM. Некоторые ATM-коммутаторы поддерживают также станции других типов (не ATM). Такие коммутаторы обеспечивают взаимодействие между ЛВС Ethernet и token ring и сетями ATM. Коммутаторы также поддерживают порты (для подключения станций и серверов) и транки (для соединения коммутаторов ATM или подключения к магистральным коммутаторам) ATM. Интерфейс между коммутаторами основан на UNI, но включает дополнительно специальные сообщения для маршрутизации и управления состоянием маршрутов. ATM Forum называетэтотинтерфейс Private Network-to-Network Interface или P-NNI.

Эмуляция ЛВС во всех вариантах состоит из двух программных частей - функции клиента используются на конечных системах, подключенных к эмулируемым ЛВС, а функции сервера - реализуются в каждой группе клиентских станций. Группа клиентов и связанный с ней сервер называются эмулируемой ЛВС (Emulated LAN или ELAN).

Протоколы ЛВС являются многоуровневыми и, следовательно, любой стандарт, обеспечивающий взаимодействие традиционных ЛВС и АТМ должен обеспечивать поддержку соответствующих уровней. В этом вопросе существующие стандарты эмуляции ЛВС существенно различаются. ATM LANE (стандарт ATM Forum) предназначен для эмуляции протоколов канального (MAC/LLC) уровня. Поскольку этот протокол занимает самый нижний для ЛВС уровень, LANE можно использовать со всеми протоколами ЛВС вышележащих уровней, включая TCP/IP, NetWare SPX/IPX, IBM SNA/LLC2. RFC 1577, с другой стороны, работает на сетевом уровне (уровень 3) и предназначен для протокола TCP/IP.

Оба варианта эмуляции ЛВС похожи по принципам работы, несмотря на различие уровней. При организации АТМ ЛВС клиентские системы пытаются вступить в контакт с сервером и зарегистрировать адресную информацию, которая содержит адрес АТМ, а также адреса канального и сетевого уровней. Сервер строит каталог адресной информации для последующего использования. По завершении регистрации клиенты и серверы переходят в режим ожидания пользовательского трафика.

Пользовательские программы, работающие на клиентских и серверных системах, функционируют в среде эмуляции ЛВС как в обычных средах традиционных локальных сетей и только коммуникационные драйверы нижних уровней связаны с АТМ. Когда программа генерирует сообщение, это сообщение передается вниз по стеку протоколов программам АТМ, прибывая к ним в форме дейтаграммы или сообщения без организации соединения на уровне два (канальном) или уровне 3 (сетевом) в зависимости от способа эмуляции ЛВС. Программы АТМ должны обеспечить эмуляцию ЛВС.

Если между отправителем и получателем будет существовать виртуальное устройство, дейтаграммы можно просто помещать в это виртуальное устройство и передавать получателю в исходной форме (дейтаграмма) для обработки на станции получателя программами АТМ и приложением. Фактически, каждый клиент АТМ поддерживает таблицу адресов канального и сетевого уровня, а же идентификаторов виртуальных устройств АТМ (VPI/VCI). Если адрес получателя найден в таблице, дейтаграмма передается соответствующему виртуальному устройству. Проблема возникает когда адрес получателя не найден - в этом случае в игру вступает сервер эмуляции ЛВС.

Клиентская система, не имеющая виртуального устройства АТМ, должна организовать его, но дейтаграмма является сообщением ЛВС и не содержит АТМ-адреса получателя. Для получения этого адреса клиент посылает сообщение своему серверу, указывая получателя дейтаграммы с помощью адреса сетевого и/или канального уровня и запрашивая соответствующий адрес АТМ. Сервер сообщает адрес, после чего клиент

организует коммутируемое соединение ATM SVC с адресатом, в которое направляется поток дейтаграмм.

Сервер также обеспечивает поддержку широковещательного и неадресованного (broadcast and unknown) трафика для клиентов, рассылающих широковещательные и групповые (multicast) дейтаграммы. Сервер в таких случаях пересылает принятые дейтаграммы всем зарегистрированным клиентам. Перед организацией SVC клиент может также использовать режим "broadcast and unknown" для рассылки дейтаграмм адресатам, для которых адреса ATM еще не получены.

Устройства традиционных ЛВС должны обмениваться данными со станциями ATM, работающими в эмулируемых ЛВС; коммутаторы обеспечивают функции proxy-клиента от имени станций традиционных ЛВС (не ATM). В этом случае станция ATM, вызывающая станцию ЛВС будет получать от сервера адрес proxy-клиента и организовывать SVC по этому адресу. Proxy-клиент будет в этом случае играть роль моста или маршрутизатора для передачи дейтаграмм нужной станции. На практике такое использование эмуляции является преобладающим, поскольку большинство настольных станций по-прежнему используют Ethernet или token ring.

Это может выглядеть как попытка создания всемирной "плоской" сети, но это не так. RFC 1577 задает ограничение на размер доменов эмуляции ЛВС - не более одной IP-подсети на домен. ATM Forum LANE не содержит такого ограничения, но практический размер домена устанавливается числом генерируемых многоадресных сообщений (с ростом этого числа растет нагрузка на сервер и клиентов). В действительности LANE представляет собой мост, а широковещательный и групповой трафик всегда является ограничивающим фактором для сетей на базе мостов.

Как связать между собой эмулируемые домены ЛВС? Лучшим способом является использование коммутаторов ЛВС. Поскольку коммутатор может одновременно работать с ATM LANE и дейтаграммами традиционных ЛВС, он может обеспечивать связь эмулируемых доменов (как подсетей IP или сегментов ЛВС).

Проблема возникает при использовании маршрутизаторов для соединения устройств ATM, использующих multimedia-приложения. Маршрутизаторы, как устройства, работающие без организации соединений, не могут обеспечивать гарантии качества обслуживания (QoS), предлагаемой коммутаторами ATM. Таким образом, маршрутизатор между двумя станциями ATM существенно ограничивает возможности связи между этими станциями (до уровня станций традиционных ЛВС). Решения на базе коммутаторов позволяют сохранить гибкость и скорость ATM.

Естественные соединения ATM требуют коммутируемого пути между адресатом и отправителем. Если оба устройства подключены к одному коммутатору, проблем не

возникает. Также просто организовать связь между устройствами, использующими услуги одного оператора или коммутаторы одного производителя. При соединении устройств в среде с разнотипным оборудованием может потребоваться использование PNNI для организации мостов между двумя или несколькими коммутаторами ATM и в тех случаях, когда ATM-соединение организуется через распределенную сеть (WAN).

Существует три варианта организации "реальных" соединений ATM через распределенную сеть:

1. Выделенная цифровая линия от оператора (T3, например) служить транком между двумя коммутаторами ATM - эти коммутаторы будут генерировать ячейки, обеспечивать сигнализацию ATM и поддерживать потоки трафика. Фактически, это вариант частной сети ATM.

2. Оператор ATM может обеспечивать виртуальный путь между парой коммутаторов. В этом случае оператор передает ячейки и принимает участие в управлении трафиком ATM, но соединенные между собой устройства управляются виртуальными устройствами как при использовании соединения по выделенной линии.

3. Может использоваться предоставляемое оператором коммутируемое соединение ATM SVC.

В первых двух вариантах ATM-коммутаторы принадлежат пользователю и должны выполнять все операции по преобразованию адресов (логические адреса, известные приложениям, конвертируются в реальные адреса ATM). В последнем варианте может потребоваться преобразование адресов оператором или, по крайней мере, использование архитектуры, поддерживающей соединений частных сетей через публичные. Одна из таких архитектур обеспечивается протоколом NHRP (маршрутизация в следующий интервал), предложенным IETF. Поскольку элементы протокола NHRP включены в базовую архитектуру стандарта ATM Forum MPOA, очевидно, что MPOA будет поддерживать управление адресами в больших сетях ATM, подключенных к системам общего пользования.

В долгосрочной перспективе ATM может полностью заменить технологии ЛВС и системы межсетевого взаимодействия в их современном виде. Сети на базе коммутаторов, в результате, будут значительно более гибкими, нежели связанные между собой ЛВС. Стоимость таких решений также может оказаться меньше. Многие пользователи верят в перспективность ATM и даже неизбежность успеха этой технологии. Однако переход к использованию ATM тормозится высокими ценами на оборудование и сложностью его использования.

Эволюция

Большинство организаций входят в одну из трех категорий с точки зрения перспектив использования ATM:

1. Организации, которые используют приложения сильно выигрывающие в результате перехода на ATM. Примером компаний этого класса являются организации здравоохранения, брокерские фирмы с большими потоками коммерческой информации, компании, занимающиеся производством видеопродукции.

2. Организации, которые могут перейти на ATM в результате агрессивной ценовой политики поставщиков услуг.

3. "Оборонительная стратегия" Организации этого типа знают, что технология ATM обеспечит им целый ряд преимуществ, но пока не планируют использовать данную технологию.

Для любой компании первым правилом эволюции ATM является *предотвращение потери средств, вложенных на этапе оценки технологии ATM*. Это означает, что при покупке сетевого оборудования сегодня нужно принимать во внимание возможность использования этого оборудования в будущей сети на базе ATM. Если от закупаемого сегодня оборудования придется потом отказываться, лучше сразу поискать другое решение.

Это правило наиболее ярко проявляется при выборе сетевых коммутаторов. Приобретаемые сегодня устройства должны обеспечивать возможность использования в системах на базе ATM. Минимальным требованием является возможность использования ATM-транков для связи между коммутаторами. Желательно также иметь в коммутаторе порт (или гнездо для его установки), позволяющий в будущем подключить настольные станции с интерфейсом ATM. Маршрутизаторы, пока не будет найдено более эффективного решения для ATM, должны использоваться как краевые устройства, обеспечивающие возможность подключения устройств традиционных ЛВС к сетям ATM. По крайней мере, такие устройства должны иметь интерфейс proxy-клиента эмуляции ЛВС.

Организации с "оборонной" стратегией, отмеченные в категории три, могут счесть наличие транкового порта ATM в коммутаторе достаточной для ближайших перспектив использования ATM (использовать не будем, но на всякий случай возьмем).

Компании, планирующие для ATM ключевую роль в своей сети, должны выбирать коммутаторы с портами ATM для подключения настольных станций. ATM обеспечивает широкий диапазон скоростей для подключения настольных станций - от 25 до 155 Мбит/с. ATM25 работает с кабельными системами категории 3 - 5 и может использоваться вместо token ring или 10BaseT для станций с высоким уровнем сетевых запросов.

Снижение цен на оборудование ATM для настольных станций играет важную роль, поскольку сегодня приложений, не способных обойтись без возможностей ATM, еще не так много. Скорей всего, пользователи первых станций ATM будут работать с одним из рассмотренных выше вариантов эмуляции ЛВС и большинство приложений будут скорее использовать эмуляцию, нежели естественные ATM API. Адаптеры ATM и коммутационные

технологии должны удовлетворять потребности пользователей в течение 5 -8 лет, а скорость отказа от традиционных технологий ЛВС будет в значительной мере определяться темпами расширения числа видеоприложений.

Понимание того, что большинство пользователей не работает с приложениями, требующими возможностей ATM зачастую служит тормозом внедрения ATM, поскольку никому не хочется тратить деньги га приобретение неиспользуемых возможностей. Использование ATM только на части станций избавит от ненужных расходов на модернизацию сети.

Если вы предполагаете начать использование ATM в настольных станциях в течение ближайшей пары лет, вам нужно выбирать коммутаторы с учетом этой перспективы. Коммутаторы должны иметь порты для подключения станций и магистральны порты 155 и 622 Мбит/сдля соединения коммутаторов. Порты ATM должны поддерживать эмуляцию ЛВС. Важно также обратить внимание на перспективы реализации в коммутаторах поддержки таких протоколов, как RFC 1577 и MPOA. Наконец, транковый интерфейс для связи с другими коммутаторами должен поддерживать стандарт PNNI.

Если оператор ATM предлагает свои услуги по разумным ценам или ваша организация планирует организовать собственную магистраль ATM, следует оценить потребности до покупки оборудования ATM. Остается ответить на вопрос "Какой тип ATM-сервиса использовать?"

Публичные или частные системы ATM будут нормально поддерживать подключение устройств frame relay через специальные преобразователи (ATM DSU/CSU). Если ваше соглашение с оператором ATM требует покупки такого оборудования для подключения других источников трафика к ATM, может оказаться более эффективной реализация сервиса frame relay на базе существующих коммутаторов и их связь с ATM через краевые устройства.

Если для подключения связывающих сети устройств (типа маршрутизаторов) к ATM вам потребуется покупать дополнительные устройства, лучше будет купить интерфейс ATM для коммутатора. Этот интерфейс можно будет использовать и после перехода на ATM, тогда как устройства DSU/CSU после такого перехода станут просто ненужными. Существует три варианта подключения ATM к коммутаторам:

1. Естественная форма ATM (ячейки) с прямым подключением цифрового транка ATM (обычно T1 или T3) к маршрутизатору. Этот тип интерфейса может поддерживать все типы сервиса ATM (включая multimedia). Такой вариант целесообразно выбирать при планировании перехода от маршрутизаторов к коммутаторам ATM.

2. DXI-форма ATM - интерфейс на основе кадров, поддерживающий только транспортный сервис ATM, ориентированный на передачу данных. Такой тип подключения хорош для систем, где не планируется замена маршрутизаторов на коммутаторы ATM.

Выбирая этот вариант, следует помнить, что некоторые операторы ATM не поддерживают DXI-сервис и может потребоваться покупка ATM DSU/CSU для преобразования DXI в ячейки ATM.

3. Интерфейс F-UNI, который представляет собой вариант интерфейса frame relay с поддержкой сигнализации ATM. Этот вариант пока распространен недостаточно широко, но может обеспечить просто и недорогой переход для маршрутизаторов, которые уже поддерживают frame relay.

При любом варианте перехода на ATM в первую очередь возникает задача организации магистралей. Организация компактных магистралей (collapsed backbone) без использования технологии ATM в таком случае будет весьма рискованным решением. Магистральные технологии при переходе на ATM приходится менять в первую очередь. Наиболее критичным при переходе на ATM будет первый шаг в сторону от традиционной коммутации ЛВС. В системах коммутации ЛВС без ATM-транков магистрали не используют технологии ATM и, следовательно, модернизация магистралей будет достаточно рискованным шагом. В идеальном случае коммутаторы ЛВС должны поддерживать магистрали ATM и других типов (например, FDDI).

Переход приложений на ATM будет постепенным. На настольных станциях ATM будет поначалу использоваться для эмуляции ЛВС и работы с набором традиционных приложений ЛВС. По мере расширения инфраструктуры ATM станет возможным связать большие группы пользователей в "чистые" сети ATM. Это позволит использовать специальные приложения, рассчитанные на качество обслуживания ATM (видео, multimedia и т.п.) или упростить работу с традиционными потоками данных за счет более высокой производительности ATM.

ATM, по мере реализации, будет делать сеть компании более гармоничной - сначала на уровне магистралей, а потом и для настольных систем. Полный переход на ATM наверняка будет определяться темпами снижения цен на порты для подключения настольных станций и адаптеры, а также реализацией поддержки возможностей в прикладных программах. Использование единой технологии для организации магистралей, подключения настольных станций и распределенных сетей может обеспечить, в конечном итоге, существенную экономию.

В долгосрочной перспективе ATM должна стать единой архитектурой внутрикорпоративных и межкорпоративных коммуникаций. Коммутируемые виртуальные устройства, используемые настольными системами могут быть расширены за счет поддержки соединений SVC операторами публичных сетей, делая ATM универсальной технологией multimedia-сетей. Протоколы типа NHRP являются средством обеспечения

универсальной связи, но в конечном итоге набор протоколов ATM для multimedia будет, по-видимому, основан на службах каталогов.

Степень воздействия универсальных multimedia-коммуникаций на бизнес достаточно трудно прогнозировать с учетом отсутствия альтернативных вариантов. Несомненно, ATM будет играть значительную роль в коммерции, здравоохранении, обучении за счет систем распространения информации. Системы ATM основаны на экономичной технологии мультиплексирования, позволяющей преодолеть барьеры, связанные с взрывным характером трафика во многих приложениях.

С учетом всех этих влияний технология ATM остается привлекательной реализацией и очевидно, что множество пользователей будут готовы перейти на ATM в ближайшем будущем. Это означает, что и ваша организация может быстро начать работу с ATM и расширять использование этой технологии для повышения эффективности работы.

2.14 Лабораторная работа № 20, 21 (4 часа)

Тема: «Настройка сетевой ОС Windows Server 2003»

2.14.1 Цель работы: изучить установку, настройку и особенности сетевой ОС Windows Server 2003.

2.14.2 Задачи работы:

1. Изучить сетевую ОС Windows Server 2003.

2.14.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Персональный компьютер.

2.14.4 Описание (ход) работы:

При планировании любого курса, связанного с использованием информационных технологий, необходимо привязывать как теоретическую часть, так и практические и лабораторные занятия к конкретным продуктам и системам — аппаратной платформе, операционным системам, системам баз данных и так далее.

При выборе программно-аппаратной платформы необходимо учитывать *целый* ряд факторов:

- имеющийся в данном вузе в наличии комплекс аппаратного и программного обеспечения;
- стоимость приобретения недостающего оборудования и ПО;
- распространенность той или иной платформы в корпоративном секторе;
- спрос на специалистов по данным технологиям в соответствующем регионе;
- квалификация и опыт преподавателей данного вуза.

С точки зрения авторов данного учебного пособия, операционные системы семейства *Windows Server* 2000/2003 являются универсальной платформой для изучения самых разных аспектов сетевого администрирования.

Приведем основные аргументы, повлиявшие на выбор авторов.

1. В любом учебном заведении имеются компьютерные классы с компьютерами, отвечающими требованиям для установки систем семейства Windows Server 2000/2003.
2. Данная система доступна учебным заведениям по различным льготным программам лицензирования — от Academic Open License до MSDN Academic Alliance и Microsoft IT Academy (кроме того, для кратковременных курсов можно использовать бесплатные 120- или 180-дневные версии системы).
3. Операционные системы Windows 2000/2003 являются основой многих корпоративных информационных систем, и имеется устойчивый спрос на специалистов по *администрированию сетей* на базе данных операционных систем.
4. Система Windows Server является универсальной платформой, на которой реализованы практически все сетевые службы, перечисленные в "Задачи и цели сетевого администрирования, понятие о сетевых протоколах и службах" — служба каталогов Active Directory, службы сетевой инфраструктуры (DNS, DHCP, WINS, маршрутизация и удаленный доступ), службы файлов и печати, службы веб-публикаций и т.д. Таким образом, при небольших затратах можно построить учебную платформу, обеспечивающую изучение всех основных сетевых служб.
5. Для подготовки вузовских преподавателей корпорация Microsoft реализует различные партнерские программы, в которых преподаватели учебных заведений могут по льготным ценам пройти обучение *администрированию сетей* на базе Windows Server.

Таким образом, курс "Сетевое *администрирование*", использующий в качестве базовой сетевой платформы системы семейства*Windows Server*, даст полезные практические знания и навыки для изучения различных сетевых служб и их администрирования.

Данное учебное пособие в качестве базового инструмента для изучения теоретической части и выполнения практических заданий рассматривает операционную систему *Windows Server* 2003 (русскую версию). Все теоретические *разделы* и задания лабораторных*работ* составлены на материале *Windows Server* 2003. Если в вашем учебном заведении базовой системой является *Windows Server*2000, то без значительных модификаций материал данного учебного пособия может быть использован и на этой платформе. В дальнейшем в тексте учебника будет преимущественно использоваться универсальный термин *Windows Server*. Если какой-либо момент будет относиться только к конкретной версии системы, то это будет оговариваться специально.

Обзор редакций и функциональных возможностей системы Windows Server 2003

Установка, настройка и использование системы *Windows Server* зависит от тех задач, которые должна выполнять конкретная*инсталляция*. Типовые задачи системы *корпорация* Microsoft объединила в виде т.н. "ролей" сервера. Все роли можно увидеть при запуске мастеров "Мастер настройки сервера" или "Управление данным сервером". Перечислим эти роли:

- файловый сервер (сервер, предоставляющий доступ к файлам и управляющий им; выбор этой роли позволит вам быстро настроить параметры квотирования и индексирования);
- сервер печати (сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров; выбор этой роли позволит вам быстро настроить параметры принтеров и драйверов);
- сервер приложений (сервер, на котором выполняются Web-службы XML, Web-приложения и распределенные приложения; при назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework; при желании вы можете добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET);
- почтовый сервер (сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту; выбрав эту роль, вы определяете домен по умолчанию для обмена почтой и создаете почтовые ящики);
- сервер терминалов (сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы; выбор этой роли приводит к установке служб терминалов, работающих в режиме сервера приложений);
- сервер удаленного доступа/сервер виртуальной частной сети (сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (*virtual private network, VPN*); выбрав эту роль, вы запустите Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote *Access Server* Setup Wizard); с помощью параметров маршрутизации и удаленного доступа вы можете разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне);
- служба каталогов (контроллер домена Active Directory — сервер, на котором работают службы каталогов и располагается хранилище данных каталога; контроллеры домена также отвечают за вход в сеть и поиск в каталоге; при выборе этой роли на сервере будут установлены DNS и Active Directory);

- система доменных имен (сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот; при выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера);
- сервер протокола динамической настройки узлов (сервер, на котором запущена служба DHCP (Dynamic Host Configuration Protocol), позволяющая автоматизировать назначение IP-адресов узлам сети; при выборе этой роли на сервере будет установлена служба DHCP и запущен Мастер создания области);
- сервер Windows Internet Naming Service (сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот; выбор этой роли приводит к установке службы WINS);
- сервер потокового мультимедиа-вещания (сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета; выбор этой роли приводит к установке служб Windows Media; эта роль поддерживается только в версиях Standard Edition и Enterprise Edition).

Microsoft *Windows Server* 2003 — самая мощная ОС для ПК. В ней реализованы совершенно новые средства управления системой и администрирования, впервые появившиеся в *Windows 2000*. Вот некоторые из них:

- Active Directory — расширяемая и масштабируемая служба каталогов, в которой используется пространство имен, основанное на стандартной Интернет-службе именования доменов (Domain Name System, DNS);
- IntelliMirror — средства конфигурирования, поддерживающие зеркальное отображение пользовательских данных и параметров среды, а также центральное администрирование установки и обслуживания программного обеспечения;
- Terminal Services — службы терминалов, обеспечивающие удаленный вход в систему и управление другими системами Windows Server 2003;
- Windows Script Host — сервер сценариев Windows для автоматизации таких распространенных задач администрирования, как создание учетных записей пользователей и отчетов по журналам событий.

Хотя у *Windows Server* 2003 масса других возможностей, именно эти четыре наиболее важны для выполнения задач администрирования. В максимальной степени это относится к *Active Directory* (речь о которой пойдет подробно в следующих главах учебного пособия), поэтому для успешной работы системному администратору *Windows Server* 2003 необходимо четко понимать структуру и процедуры этой службы.

Со способами решения административных задач теснейшим образом связана и *архитектура* системы безопасности *Windows Server*2003. *Active Directory* и административные шаблоны позволяют применять параметры безопасности ко всем рабочим

станциям и серверам компании. Иными словами, вы настраиваете защиту данных не каждого конкретного компьютера, а всего предприятия в целом.

Роли сервера по-разному реализуются в различных редакциях системы. Перечислим редакции ОС *Windows Server* 2003 и рассмотрим их краткие характеристики.

Windows Server 2003 Standard Edition. Надежная сетевая *операционная система*, реализующая базовый набор сетевых служб, разработана для предоставления служб и ресурсов другим системам в сети, является идеальным выбором для предприятий малого бизнеса и отдельных подразделений крупных организаций.

Windows Server 2003 Enterprise Edition. Расширяет возможности *Windows Server* 2003 *Standard Edition*, обеспечивая поддержку служб кластеров. В ней также поддерживаются 64-разрядные процессоры Intel Itanium, *оперативная память* с возможностью "горячей" замены и *неоднородный доступ к памяти* (nonuniform *memory* access, *NUMA*). Эта версия поддерживает до 32 Гбайт оперативной памяти на процессорах x86, до 512 Гбайт оперативной памяти на процессорах Itanium и до 8 центральных процессоров. Разработана для удовлетворения общих ИТ-требований предприятий любого размера, предназначена для приложений, веб-служб и поддержки сетевой инфраструктуры и обеспечивает высокую *надежность*, *производительность* и превосходные экономические показатели.

Windows Server 2003 Datacenter Edition.Самыйпроизводительный *Windows-сервер*. Эта версия поддерживает более сложную кластеризацию и способна работать с большими объемами оперативной памяти — до 64 Гбайт на процессорах x86 и до 512 Гбайт на процессорах Itanium. Минимальное количество процессоров для работы Datacenter *Edition* — 8, максимальное — 32. Разработана для ответственных бизнес-приложений, требующих масштабируемости и доступности высокого уровня.

Windows Server 2003 Web Edition. Данная редакция предназначена для использования в качестве веб-сервера (для запуска служб*Web* при развертывании *Web*-узлов и *Web*-приложений). Для решения этих задач в данную версию включены Microsoft *.NET*Framework, Microsoft *Internet Information* Services (*IIS*), *ASP.NET* и функции для равномерного распределения нагрузки на *сеть*. Многие другие функции, в частности *Active Directory*, в ней отсутствуют. Версия *Windows Server* 2003 *Web Edition*, поддерживает до 2 Гбайт оперативной памяти и до двух центральных процессоров.

Все версии поддерживают одни и те же базовые функции и средства администрирования. Т. е. методики, описанные в этом учебном пособии, можно применять независимо от того, какой версией *Windows Server* 2003 вы пользуетесь. Помните, что в версии *WebEdition* нет *Active Directory*, поэтому *сервер*, работающий под управлением этой

версии, нельзя сделать контроллером домена. Он, тем не менее, может быть частью домена *Active Directory*.

Различия данных редакций в поддержке сетевых служб и выполнении отдельных ролей наглядно представлены в табл. 2.1.

Таблица 2.1.

Роль, служба, компонента или поддержка аппаратуры	**Web Edition**	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**
Минимальное количество процессоров				8
Максимальное количество процессоров	2	4	8	32
Максимальный объем оперативной памяти (ГБ)	2	4	32(для серверов на базе процессора x86) 512(для серверов на базе процессора Itanium)	64(для серверов на базе процессора x86) 512(для серверов на базе процессора Itanium)
Поддержка "горячего" добавления памяти			Да	Да
Службы факсов		Да	Да	Да
Службы для Macintosh		Да	Да	Да
Службаудаленнойустановки (RIS, *Remote Installation* Services)		Да	Да	Да
Роль контроллера домена		Да	Да	Да
Сервер, член домена	Да	Да	Да	Да
Службысертификатов (PKI, Public Key Infrastructure)	Частично	Да	Да	Да
Службы терминалов		Да	Да	Да
Управление посредством Remote Desktop Protocol	Да	Да	Да	Да
Поддержка виртуальных частных сетей (VPN, Virtual Private Networking)	Частично	Да	Да	Да
Служба Internet *Authentication Service* (IAS)		Да	Да	Да
Поддержка сетевых мостов (network bridging)		Да	Да	Да

Предоставление общего доступа в Интернет (*ICS*, Internet Connection Sharing)	Да	Да		
Балансировка сетевой нагрузки (NLB, Network*Load Balancing*)	Да	Да	Да	Да
Служба кластеров (Cluster Service)		Да	Да	
Максимальное количество узлов в кластере		8	8	
Службавеб-публикаций (IIS, Internet Information Services)	Да	Да	Да	Да
Служба потокового мультимедиа-вещания (Windows Media Services)	Да	Да	Да	

Для выполнения упражнений при изучении курса "Сетевое *администрирование*" наиболее подходящей редакцией является редакция*Standard Edition*.

Планирование приобретения и установки системы

При планировании приобретения и установки сервера (или нескольких серверов) службе ИТ любой компании или организации необходимо решить целый комплекс задач:

1. определить набор задач, возлагаемых на каждый сервер (сервер сетевой инфраструктуры, сервер службы каталогов, сервер файлов/печати, сервер удаленного доступа, сервер электронной почты, сервер баз данных и т.д.);
2. определить предполагаемую нагрузку на сервер, исходя из выполняемых ими ролей и количества пользователей, которые будут работать с сервером;
3. исходя из полученной информации, определить аппаратную конфигурацию сервера (тип и количество процессоров, объем оперативной памяти, параметры дисковой подсистемы, сетевые адаптеры и пр.) и редакцию операционной системы (Standard, Enterprise, Datacenter, Web);
4. спланировать процедуру установки и параметры системы (будет ли производиться модернизация системы с предыдущей версии или новая установка, как сконфигурировать дисковую подсистему, определить сетевые параметры и т.д.).

В табл. 2.2 приведены минимальные требования для установки системы Windows Server 2003, позаимствованные из источников [4–5].

Таблица 2.2.

Аппаратные компоненты	**Web Edition**	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**
Рекомендуемая частота процессора (МГц)	550	550	773	773
Рекомендуемый объем оперативной	256	256	256	1024

памяти (МБ)				
Пространство на диске для установки (ГБ)	1,5	1,5	1,5	1,5

Подчеркнем, что данные требования относятся только к установке системы и ее запуску, без учета нагрузки, которая будет возложена на систему. Данные параметры могут быть ориентиром для преподавателей, ведущих курс "Сетевое администрирование", при планировании аппаратной конфигурации компьютеров в том классе, где будут проводиться лабораторные занятия. При планировании конфигурации сервера для реальной рабочей нагрузки в компании необходимо изучать специальные указания для планирования серверов, выполняющих конкретные роли.

Установка и начальная настройка системы

После того как определены роли, выполняемые сервером, его аппаратная *конфигурация*, редакция системы, можно приступить к установке операционной системы на сервере.

Если выполняется установка поверх предыдущей версии системы *Windows Server*, то обязательно нужно выполнить следующие предварительные действия:

1. сделать резервные копии всех данных, хранящихся и обрабатываемых на данном сервере;
2. если на работающем сервере имеются "зеркальные" дисковые конфигурации, то необходимо "разбить" зеркала;
3. отключить подключенные к серверу кабели, управляющие источником бесперебойного питания;
4. удалить программное обеспечение сторонних разработчиков (особенно это относится к сторонним программам сжатия дискового пространства, а также к антивирусным программам).

Сама процедура установки в деталях описана в книгах [4–5]. В данном пособии уделим особое внимание наиболее существенным моментам данного процесса.

Выбор режима установки

Установку системы Windows Server можно производить в одном из трех режимов:

- ручная установка, в процессе которой администратор отвечает на все вопросы мастера установки системы;
- полуавтоматическая установка (с минимальным участием администратора в процессе установки);
- автоматическая установка.

В настоящем пособии мы подробно рассмотрим ручную установку системы.

Выбор носителя дистрибутива системы

Запуск программы установки можно производить с дистрибутива, размещенного на различных носителях и различными способами:

- с установочного CD (при загрузке компьютера с данного компакт-диска);
- с установочного CD (при иной загруженной системе на данном сервере);
- с дистрибутива, размещенного на жестком диске данного сервера;
- с дистрибутива, размещенного в сети.

Первый способ предпочтителен в том случае, когда производится установка на новом сервере, на котором не было установлено никакой системы, или когда необходимо удалить имеющуюся установку и произвести иное разбиение разделов и томов на жестких дисках.

Все другие способы будут предпочтительнее в случаях модернизации имеющейся операционной системы или при установке системы в другие разделы жестких дисков для многовариантной загрузки компьютера (данная ситуация наиболее вероятна в учебном заведении, когда компьютерный класс используется для различных курсов).

Процесс установки системы

1. Запуск мастера установки системы.

   Если производится установка при загрузке компьютера с установочного CD, то после появления меню для выбора редакции системы (Standard, Enterprise, Web) администратор выбирает нужную редакцию и начинается текстовый этап установки системы.

   Если производится установка из работающей системы (для модернизации или установки системы в другой раздел жесткого диска), то вначале нужно найти путь к мастеру установки (нужно найти папку с названием I386 в дистрибутиве с нужной редакцией ОС) и затем запустить мастер (файл winnt32.exe). Например, если система устанавливается с дистрибутива, размещенного на жестком диске компьютера, то путь к папке с мастером может быть таким:D:\Server\RUSSIAN\STANDARD\I386.

   Следует помнить, что мастер установки нужно запускать с учетной записью, имеющей права администратора в работающей операционной системе.

2. Сбор информации о системе и анализ конфигурации.

   На данном этапе мастер установки проверяет, можно ли произвести модернизацию системы или только новую установку, и предлагает администратору сделать нужный выбор (рис. 1).

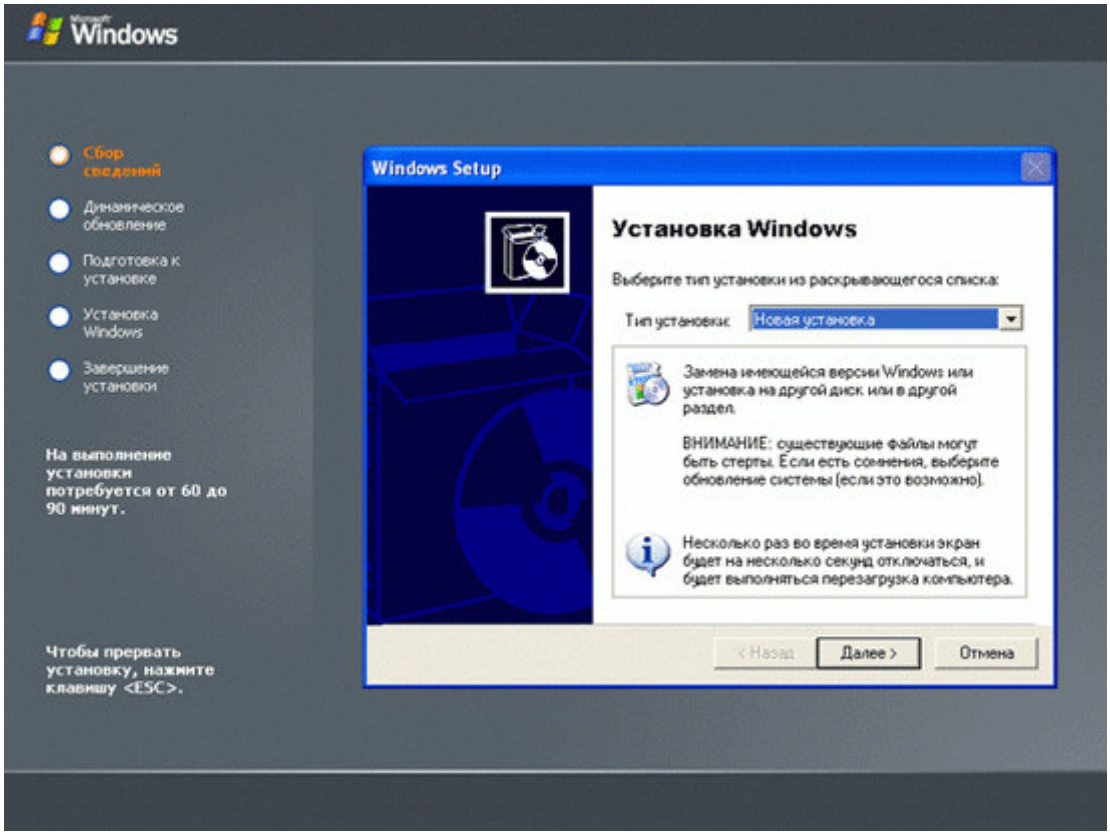


Рис. 1. Установка

Затем запрашивается ключ (Product Key) для установки системы (рис. 2). На иллюстрации изображен условный ключ, в реальной установке в каждом учебном заведении будет свой ключ.

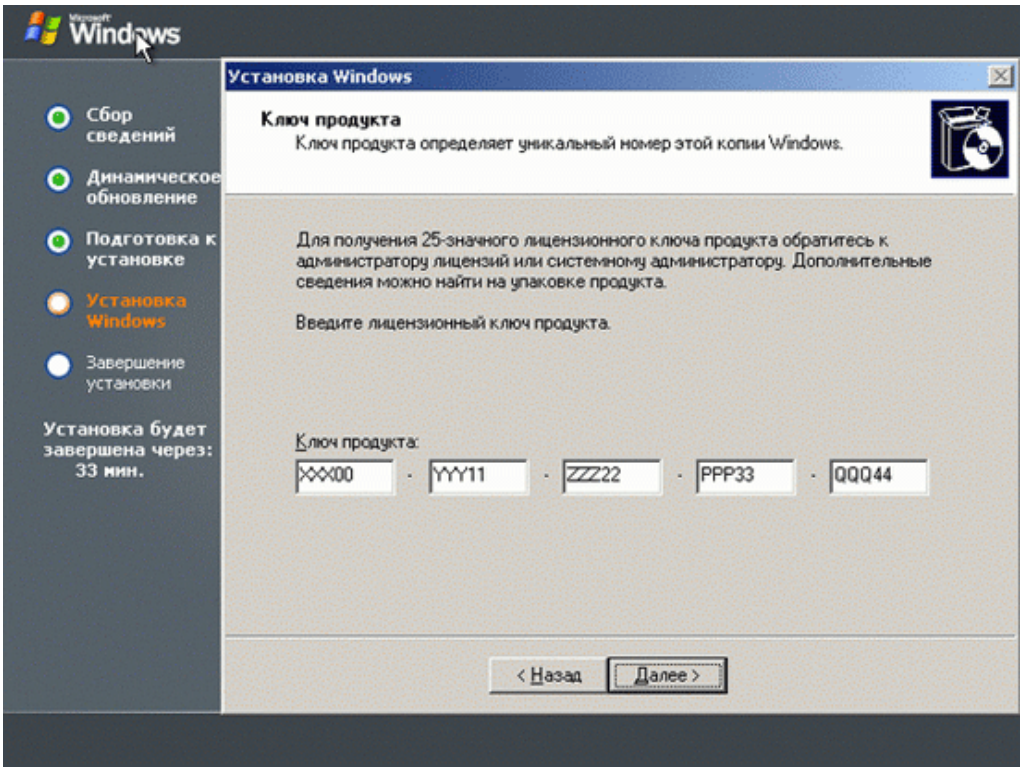


Рис. 2. Ввод ключа продукта

Затем необходимо задать параметры о дополнительных возможностях установки (рис. 3). При установке с CD рекомендуем нажать кнопку "Дополнительные параметры" и поставить галочку у параметра "Копировать все файлы с установочного компакт-диска" (это позволит в дальнейшем при добавлении новых компонент системы обходиться без компакт-диска, все нужные файлы будут скопированы на жесткий диск компьютера).

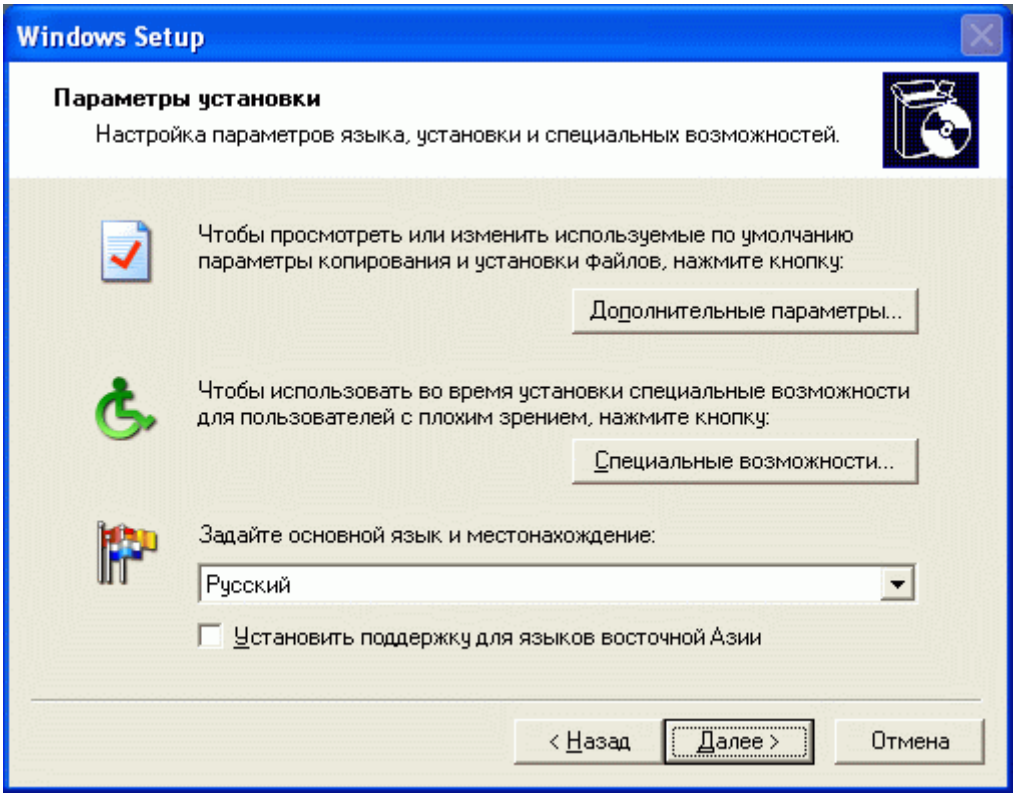


Рис. 3. Дополнительные параметры

Затем задается вопрос об использовании файловой системы (рис. 4). Рекомендуем оставить тот вариант, который предлагает система.

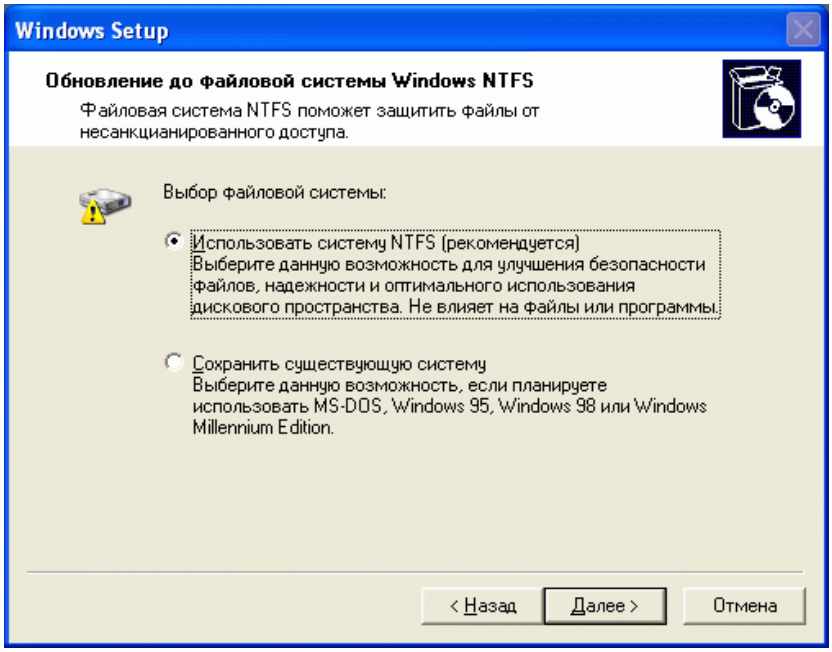


Рис. 4. Выбор файловой системы

Далее мастер предлагает загрузить из Интернета обновления системы (рис. 2.5). Несмотря на то что система по умолчанию предлагает вариант "Загрузить обновленные файлы установки", мы рекомендуем выбрать "Пропустить этот шаг …".

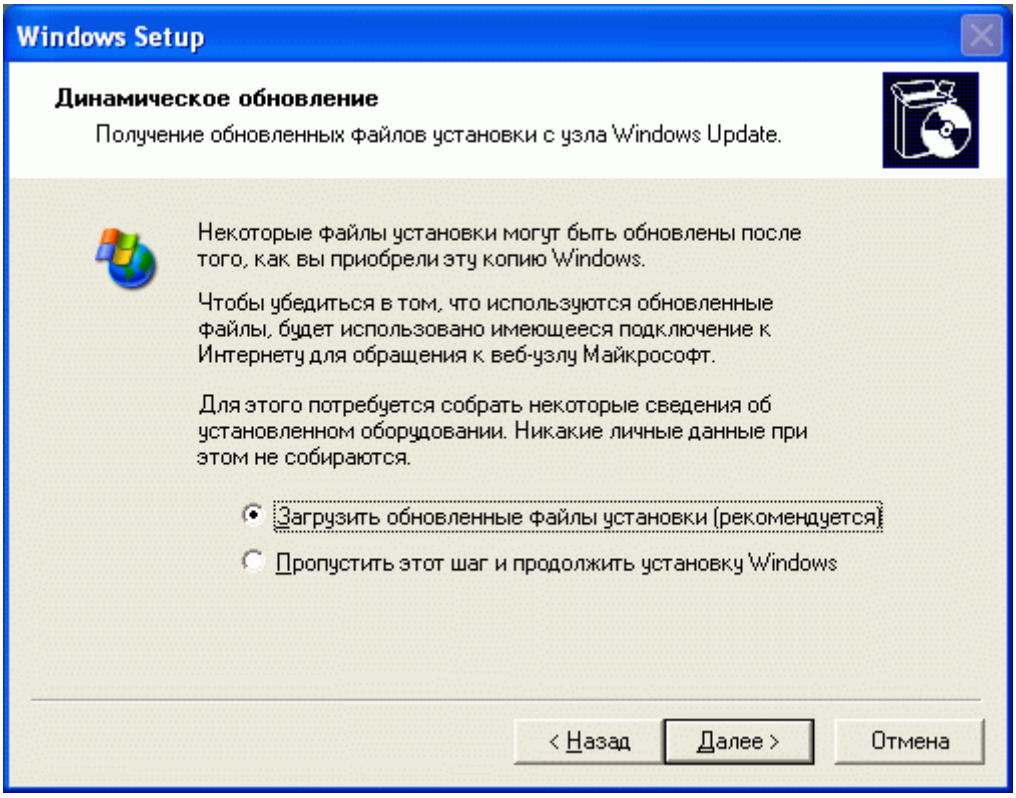


Рис. 5. Динамическое обновление

После этого начинается процесс копирования установочных файлов на компьютер (рис. 6). По его окончании система будет перезагружена, и начнется текстовый этап процесса установки системы.

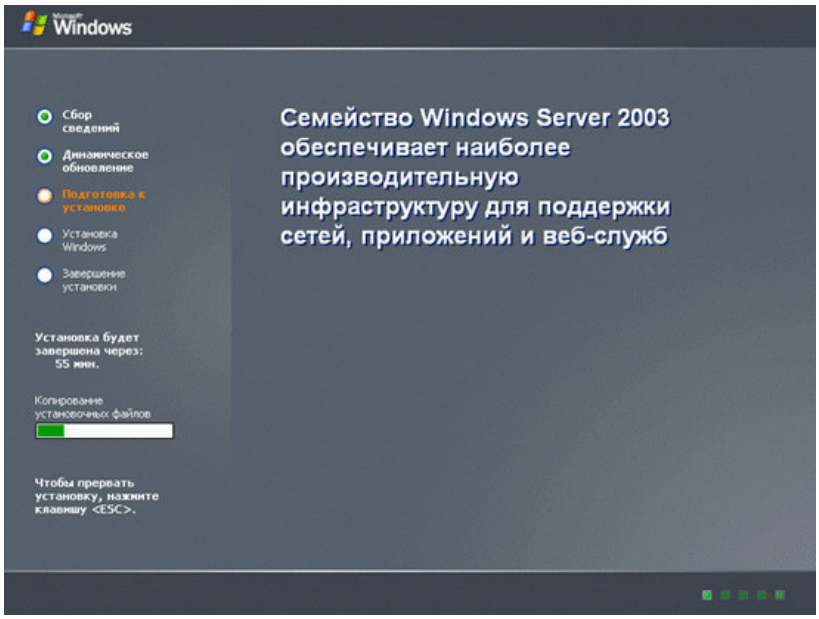


Рис. 6. Текстовый этап установки системы

Напомним, что при загрузке с установочного компакт-диска после выбора редакции операционной системы сразу начинается текстовый этап установки.

Если в вашем сервере установлен дисковый контроллер, драйвер которого отсутствует в базовом наборе драйверов системы, на данном этапе обязательно нужно нажать клавишу F6, чтобы в дальнейшем программа установки предложила вам вставить в дисковод для флоппи-дисков дискету от производителя контроллера с драйверами для данного дискового контроллера.

После этого появляется экран с выбором вариантов (рис. 7):

- начать установку системы (для этого надо нажать клавишу ВВОД/Enter);
- приступить к восстановлению поврежденной системы с помощью консоли восстановления (клавиша R);
- выйти из программы установки, прервав данный процесс (клавиша F3)

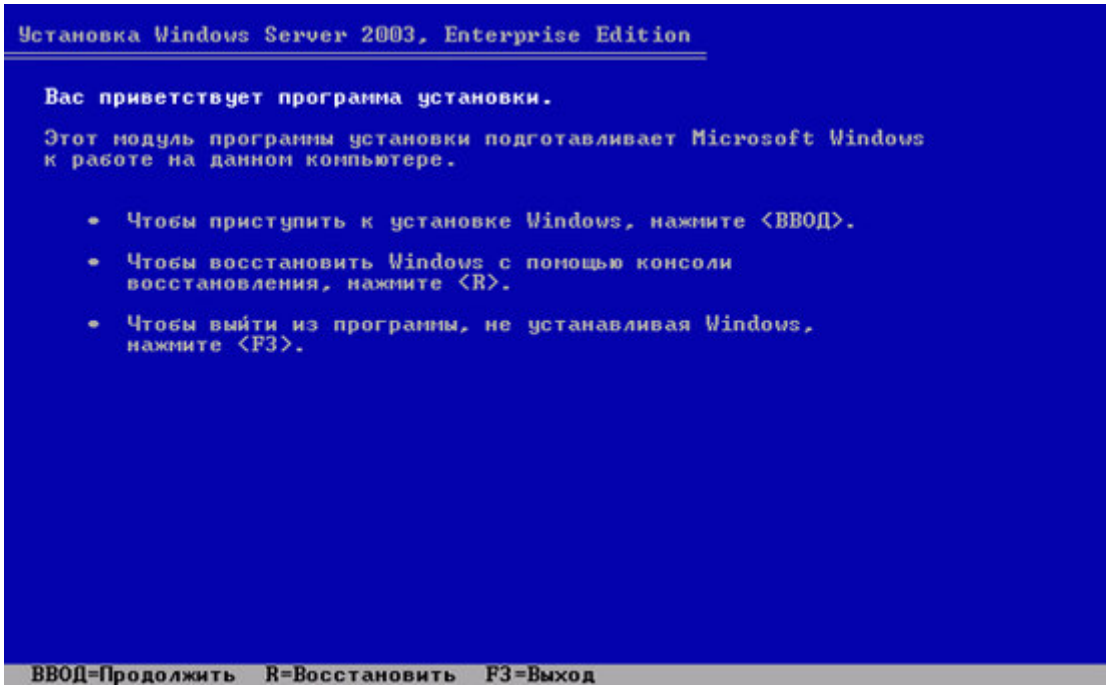


Рис. 7. Лицензионное соглашение

На следующем шаге установки необходимо прочитать Лицензионное соглашение. Если вы принимаете данное соглашение необходимо нажать F8, если не принимаете – необходимо нажать ESC.

После программа установки предлагает выбрать раздел, в который будет производиться установка системы (рис.8). Можно выбрать существующий раздел, создать новый раздел в неразмеченной области, удалить часть имеющихся разделов.

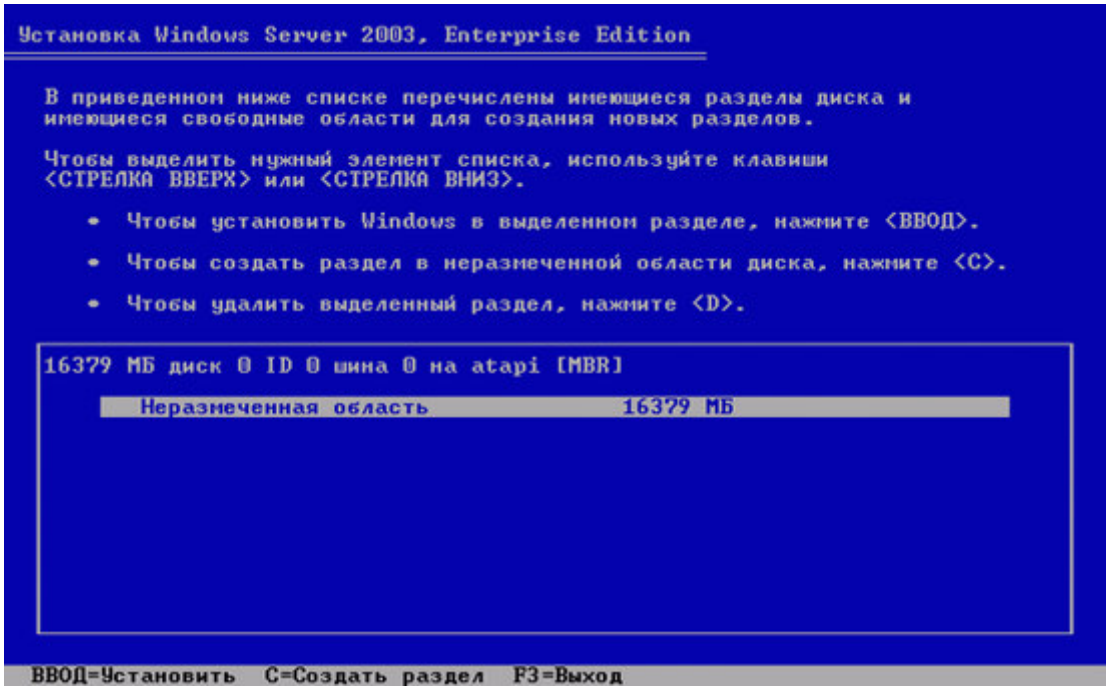


Рис. 8. Выбор места установки

В данном примере в неразмеченной области создается раздел размером 5000 МБ (рис. 9).

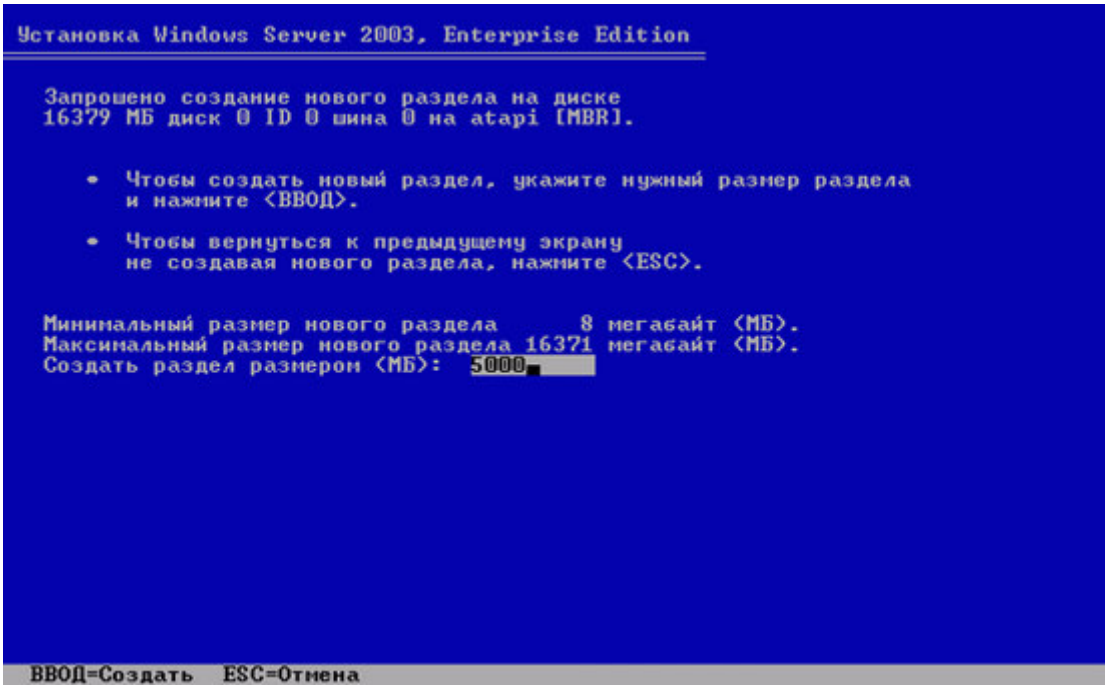


Рис. 9.

Здесь виден результат создания раздела (рис. 2.11). Нажимаем ВВОД/Enter для запуска установки системы в выбранный раздел.

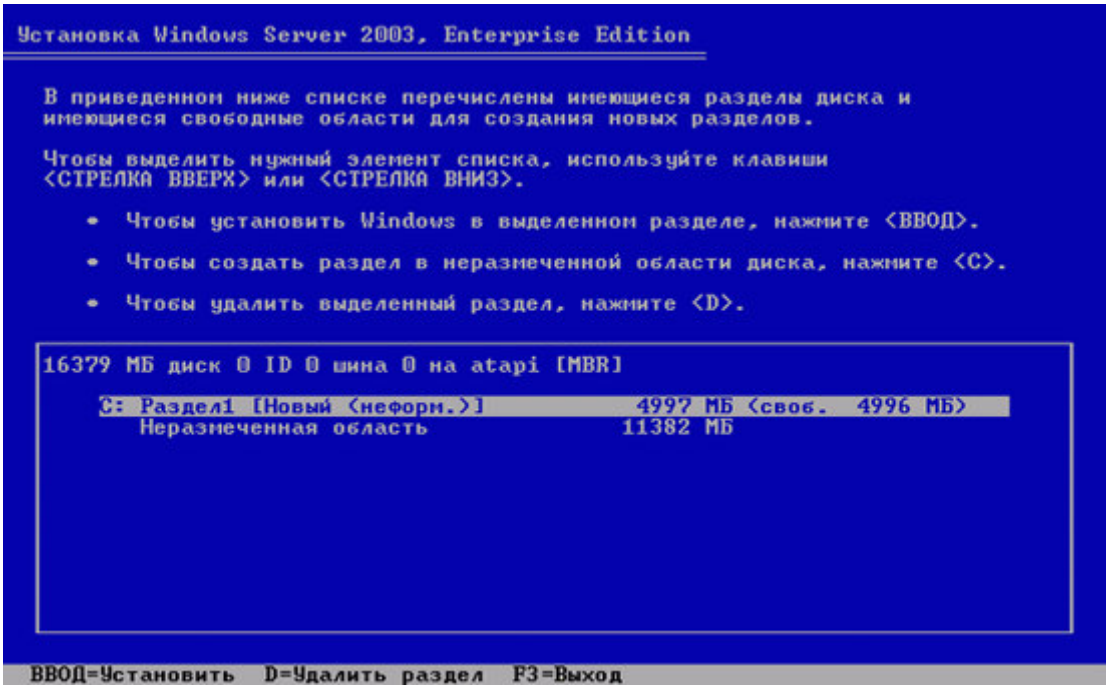


Рис. 10.

Выбираем вариант "Форматировать раздел в системе NTFS (Быстрое)" и продолжаем установку (рис. 11).

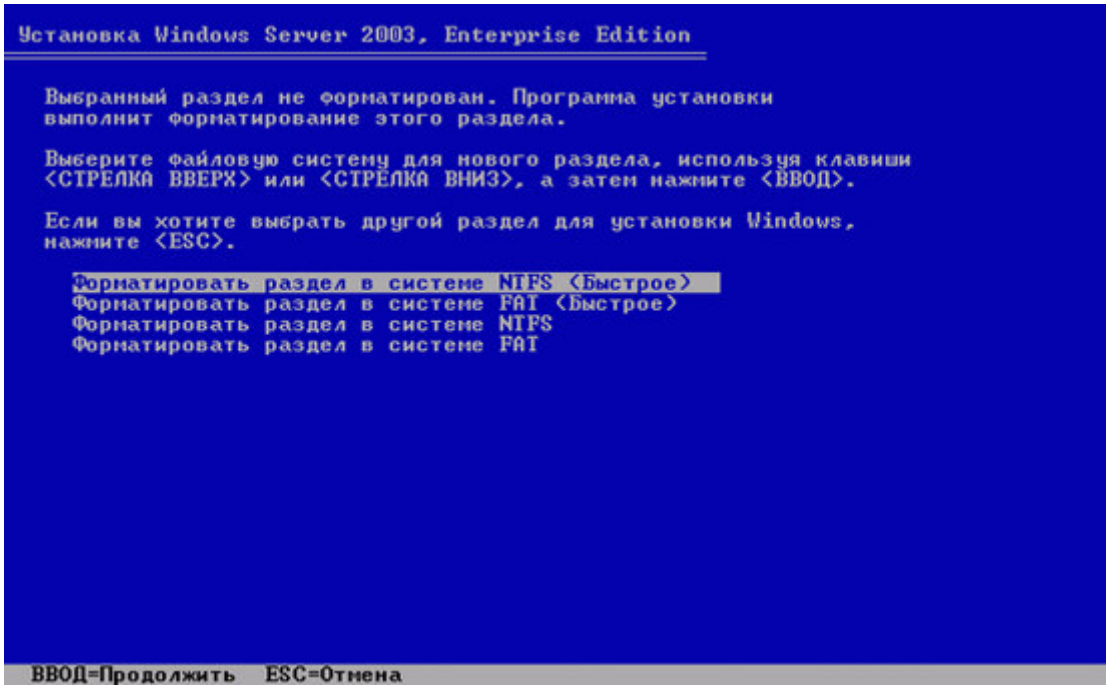


Рис. 12.

Программа установки форматирует выбранный раздел (рис. 13.).

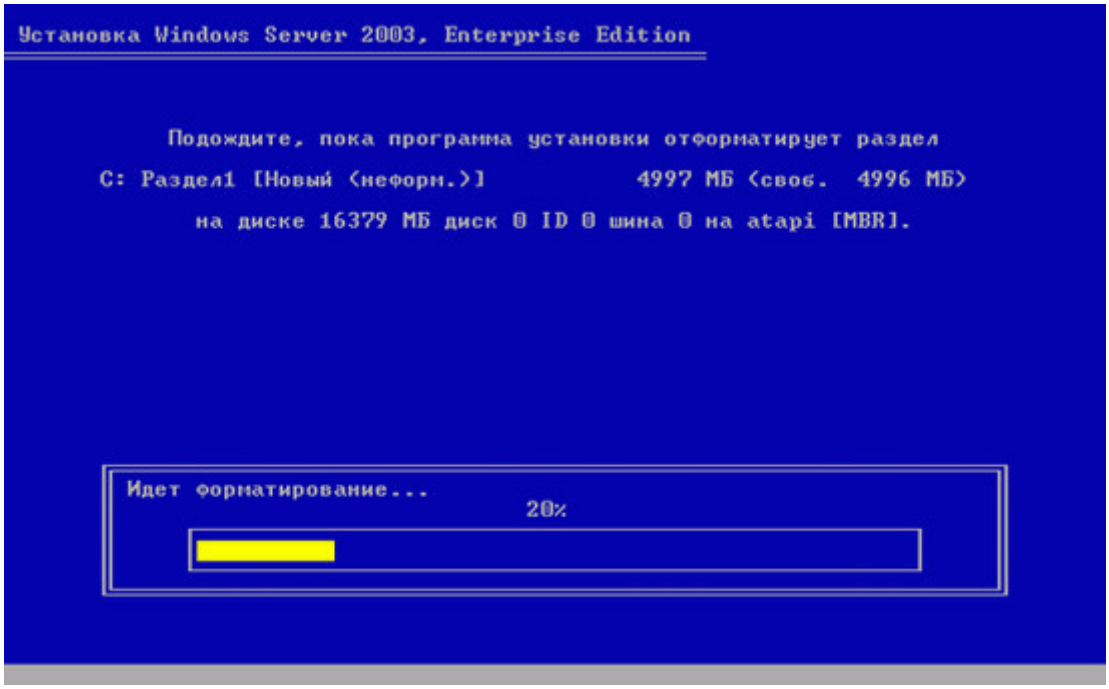


Рис. 13.

После форматирования программа установки копирует необходимые файлы на жесткий диск (рис. 14).

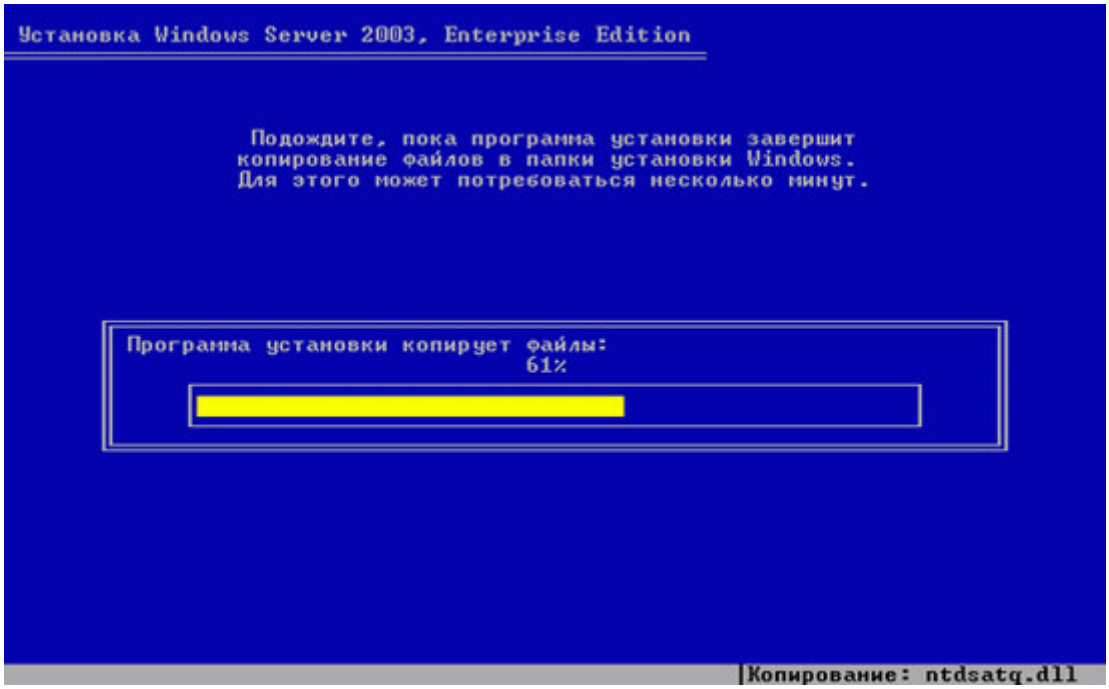


Рис.14.

После завершения копирования производится перезагрузка компьютера, и начинается графический этап установки системы.

Графический этап установки системы.

Начальный экран графического этапа — опрос оборудования и поиск имеющихся аппаратных компонент сервера. На данном этапе будут обнаружены все устройства Plug and Play, и, если в дистрибутиве системы имеются драйверы для этих устройств, то они будут установлены (рис. 2.15).

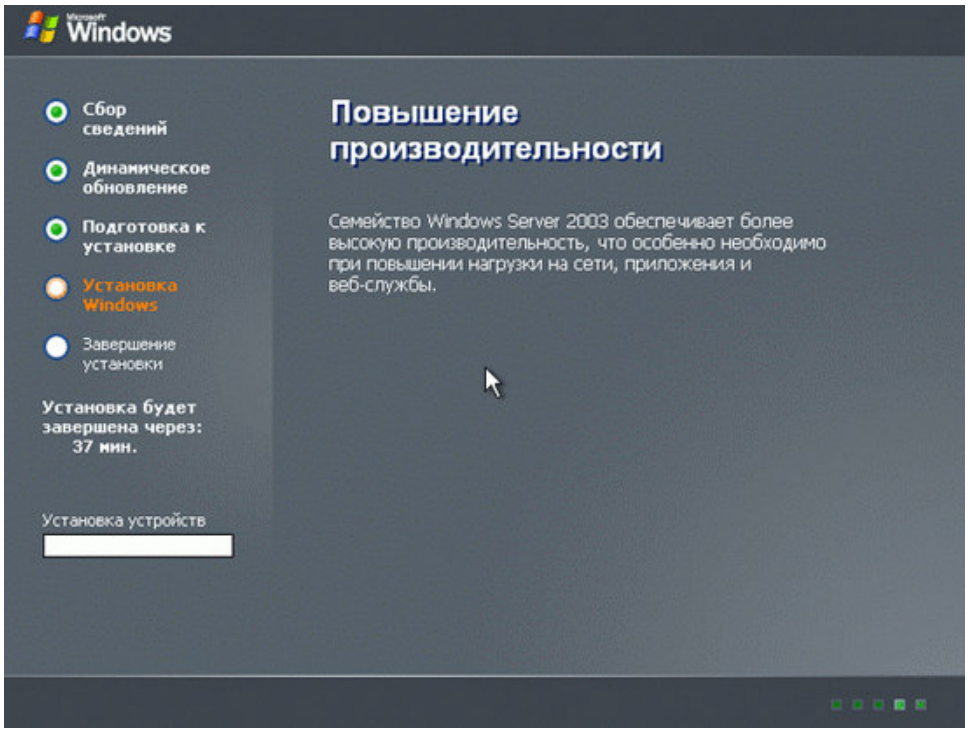


Рис. 15.

Далее — настройка языков и региональных стандартов (рис. 2.16). Если вам не надо изменять комбинацию клавиш для переключения между английской и русской раскладками клавиатуры, то можете нажать кнопку "Далее". Рекомендуем нажать кнопку "Состав" и настроить язык ввода по умолчанию — "Английский".

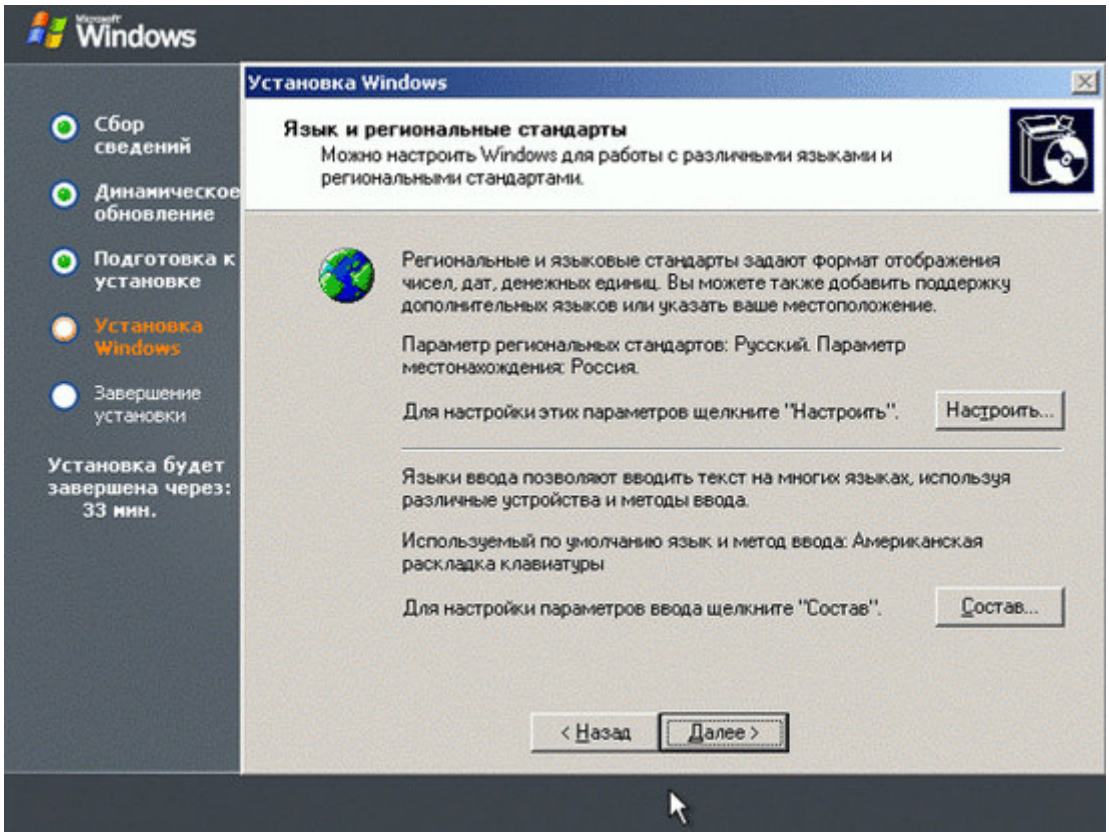


Рис. 16.

Следующий экран — настройка принадлежности программ (рис. 17). Здесь необходимо ввести имя пользователя, производящего установку, и название организации, которая приобрела данную копию системы (в учебном классе можно выбрать общее для всех имя пользователя и название учебного заведения).

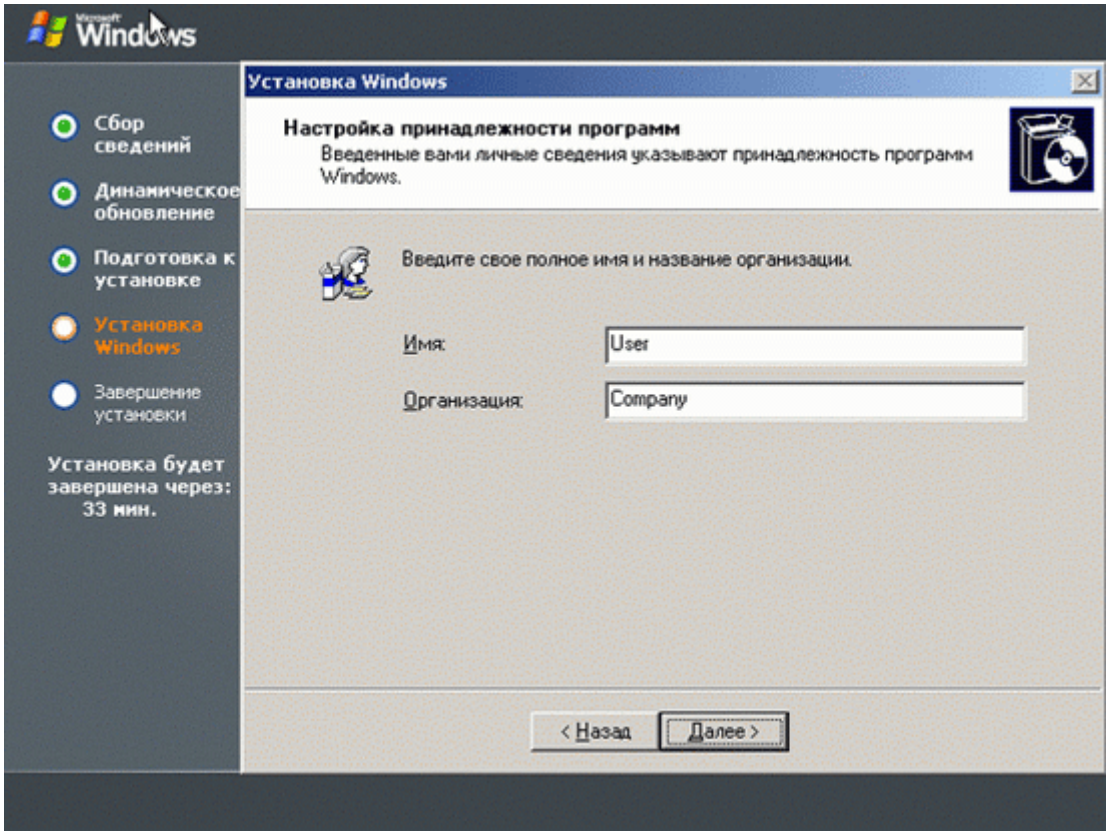


Рис. 17.

Затем повторный (если система не устанавливается с загрузочного CD) ввод ключа продукта (рис. 2.18). Снова напомним, что на иллюстрации изображен "условный" установочный ключ. Настоящий ключ — на том установочном комплекте, который вы приобрели по одной из программ лицензирования для учебный заведений.

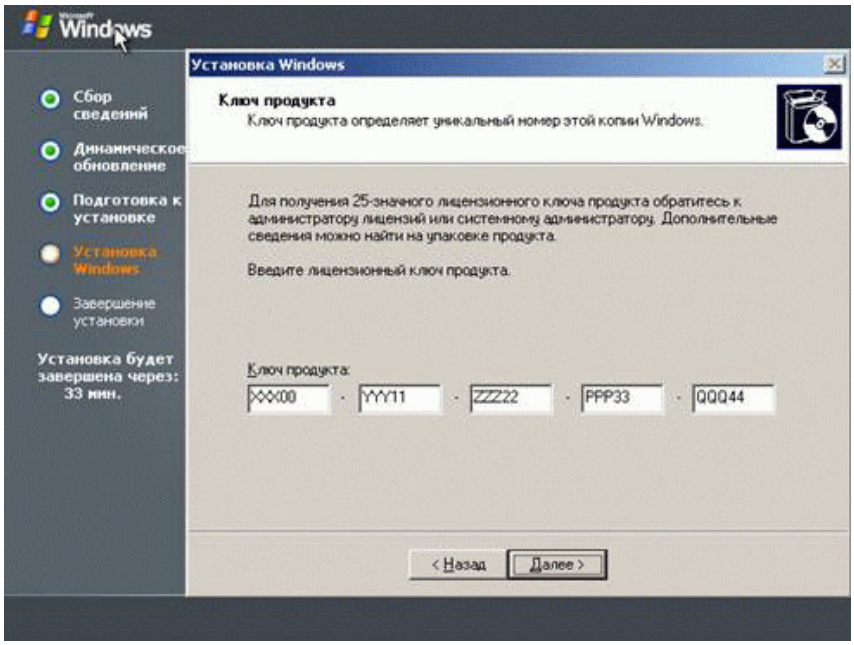


Рис. 18.

Теперь необходимо задать режим лицензирования клиентских подключений и количество лицензий (рис. 19). Режим лицензирования по умолчанию — "На сервер". При данном режиме система будет контролировать количество одновременных подключений к

данному серверу, не отслеживая имен пользователей или компьютеров, с которых производятся данные подключения. При режиме лицензирования "На устройство или на пользователя" при каждой попытке установить сеанс работы с системой система будет обращаться к доменному серверу лицензий и проверять, имеется ли лицензия у данного пользователя на работу с данным сервером. Если лицензия имеется, то сеанс работы будет установлен. Если лицензии нет, то сначала будет произведена попытка выдать новую лицензию для пользователя и записать ее в БД сервера лицензий (после чего будет установлен сеанс работы с сервером). Если же лимит лицензий исчерпан, пользователю будет отказано в доступе к данному серверу. Начальное количество лицензий – 5.

Для данного учебного курса необходимо оставить настройки по умолчанию.

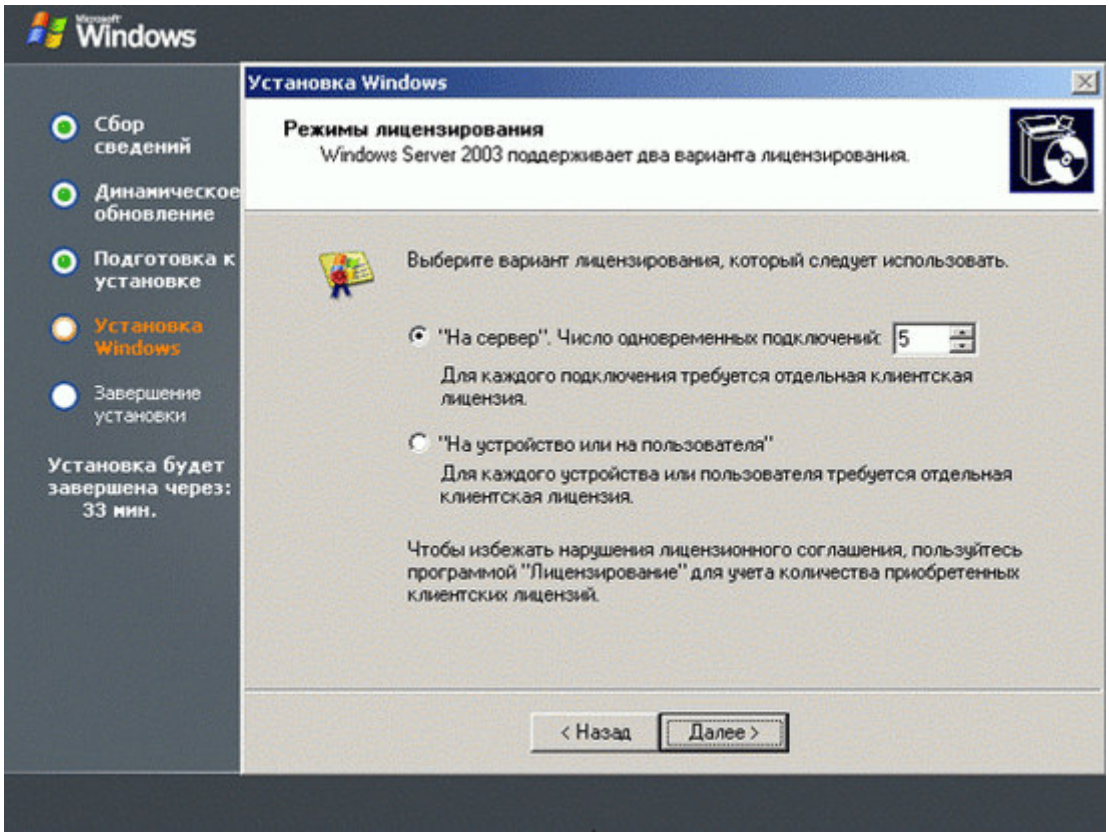


Рис. 19.

Следующий экран — выбор имени сервера и пароля для встроенной учетной записи "Администратор" данного сервера (рис .20). На иллюстрации выбрано имя DC1. Во время лабораторных занятий студенты, изучающие данный курс, будут назначать имена своих серверов в соответствии с методическими указаниями для лабораторных занятий. Пароль администратора также назначается в соответствии с данными указаниями. Набор требований к паролям учетных записей обсуждается дальше в данном курсе. Сейчас приведем основные требования к паролю:

- длина пароля не менее 8 символов;

- пароль не должен содержать имя пользователя (ни имя учетной записи, ни само имя или фамилию),а также имена его родных и близких, клички домашних животных, номера телефонов и пр. персональную информацию;
- буквы, входящие в пароль, должны быть как в нижнем, так и в верхнем регистре;
- в пароль должны входить знаки препинания и специальные символы (например, $, &, #, @ и др.).

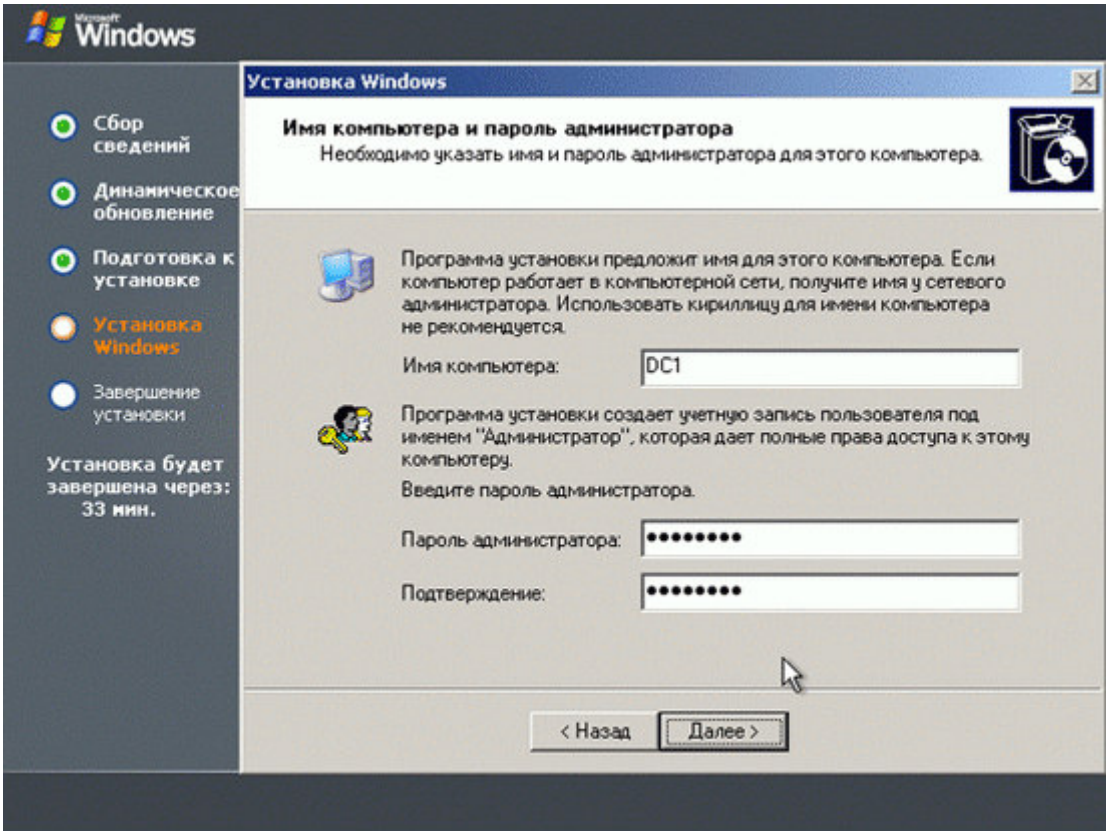


Рис. 20.

Следующий шаг — установка даты, времени и часового пояса (рис. 21). Необходимо установить данные параметры в соответствии с вашим регионом и вашим временем.

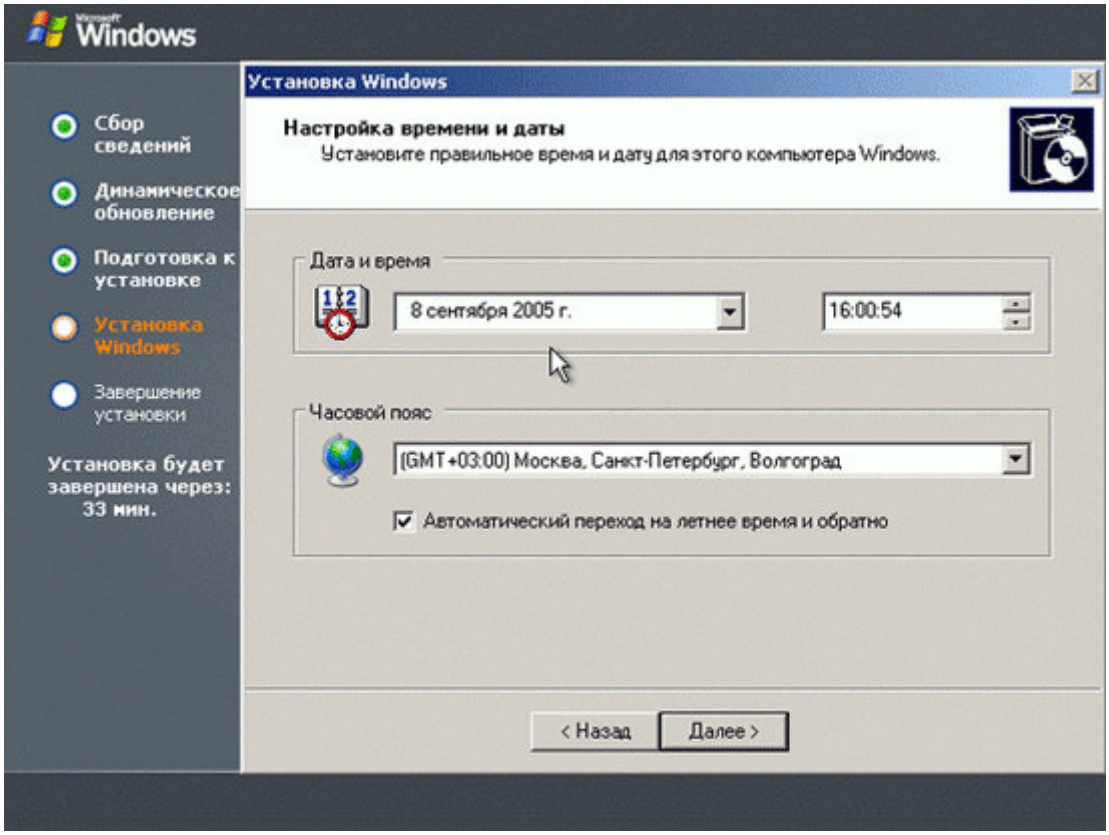


Рис. 21.

Далее — экран установки и настройки сетевых компонент (рис. 22).

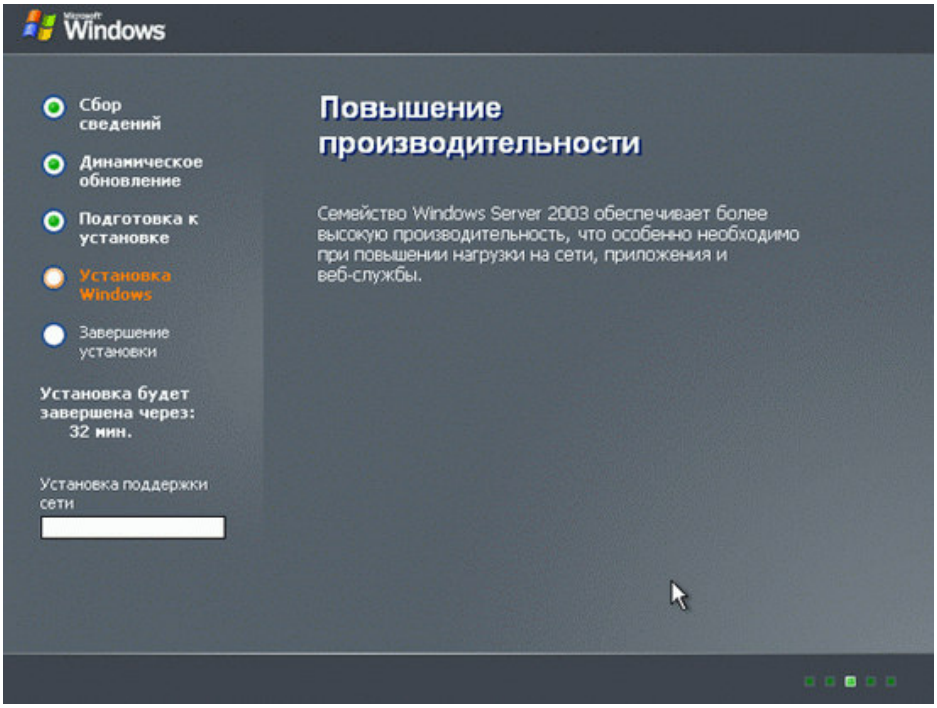


Рис. 22.

На этом этапе для каждого из сетевых адаптеров, установленных в сервере и опознанных системой, будет установлены либо "Обычные параметры", подразумевающие включение клиента для сетей Microsoft, предоставление *совместного доступа к файлам* и принтерам данного сервера и установку протокола TCP/IP с настройкой параметров данного

протокола от сервера DHCP или при помощи технологии APIPA. Выберем "Особые параметры" и изменим только настройку TCP/IP — зададим IP-адрес сервера вручную (рис. 23).

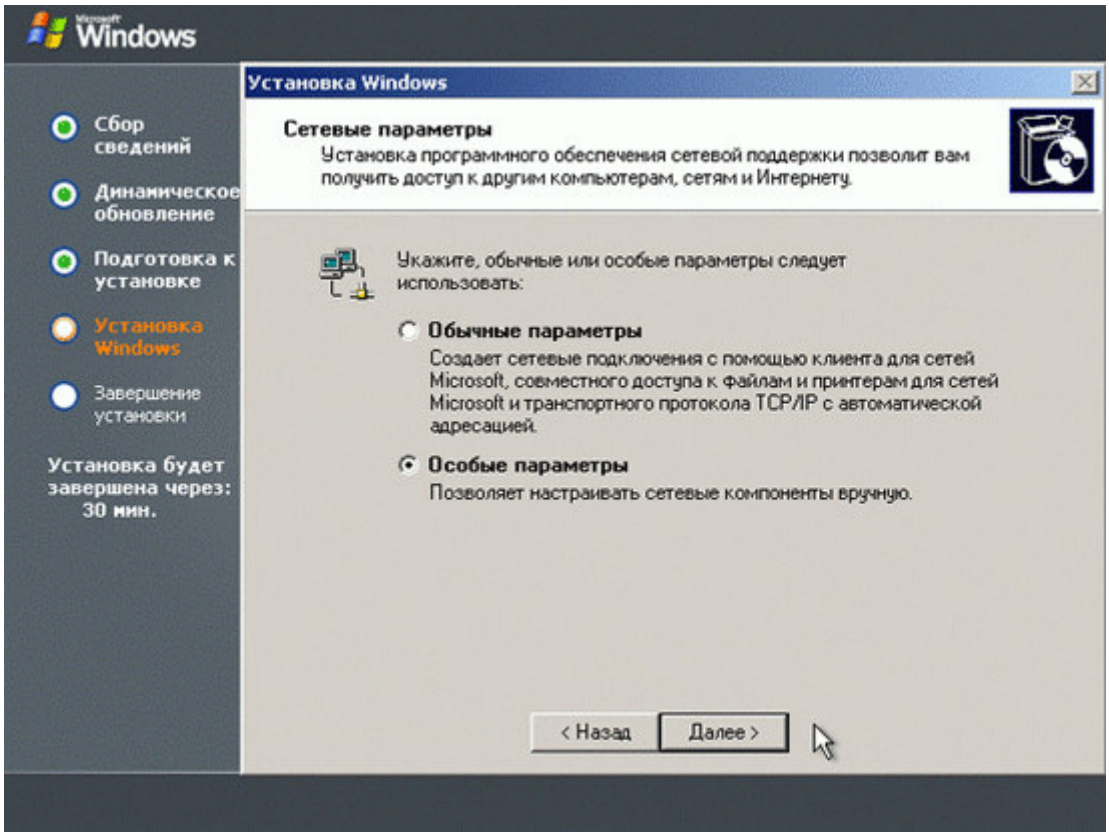


Рис. 23.

Установим параметры, как показано на рис. 24. В методических указаниях для лабораторных работ описана схема назначения имен и IP-адресов для серверов компьютерного класса.

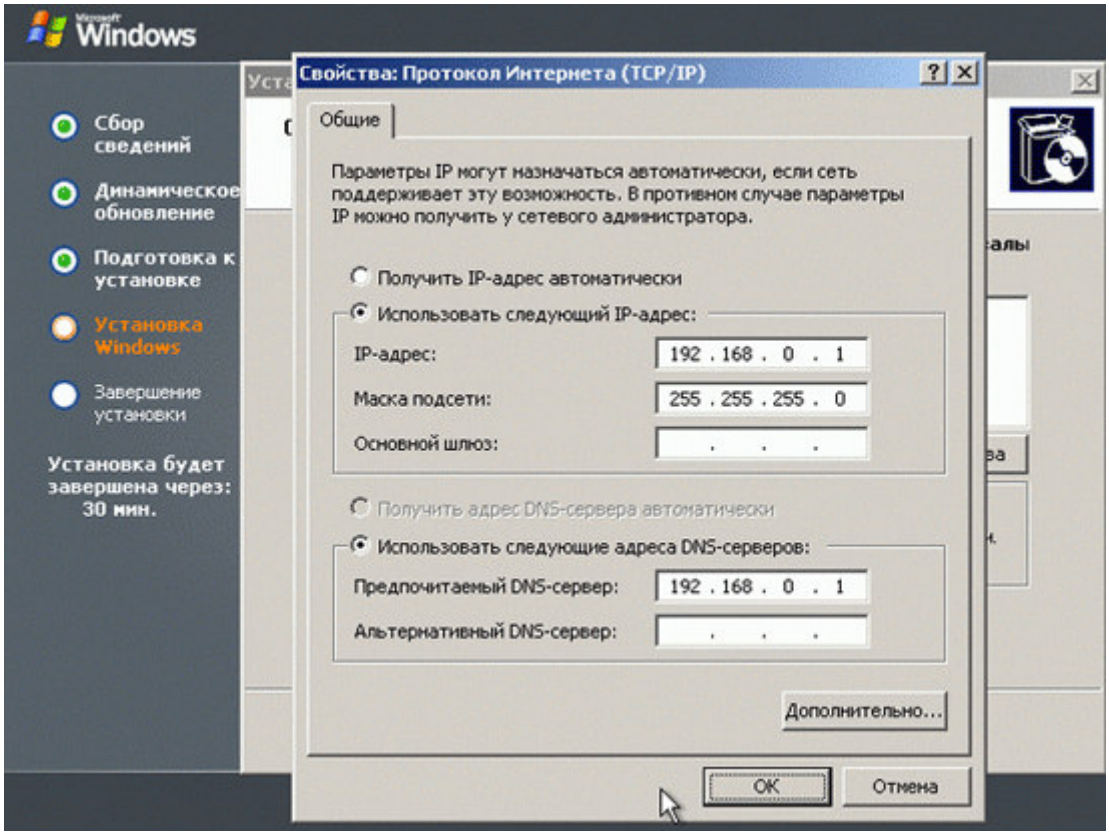


Рис. 24.

После настройки сетевых компонент программа установки предлагает оставить компьютер в рабочей группе WORKGROUP (имя рабочей группы можно на этом этапе изменить) или включить в домен корпоративной сети (рис. 2.25). На данном этапе оставим данный параметр по умолчанию.

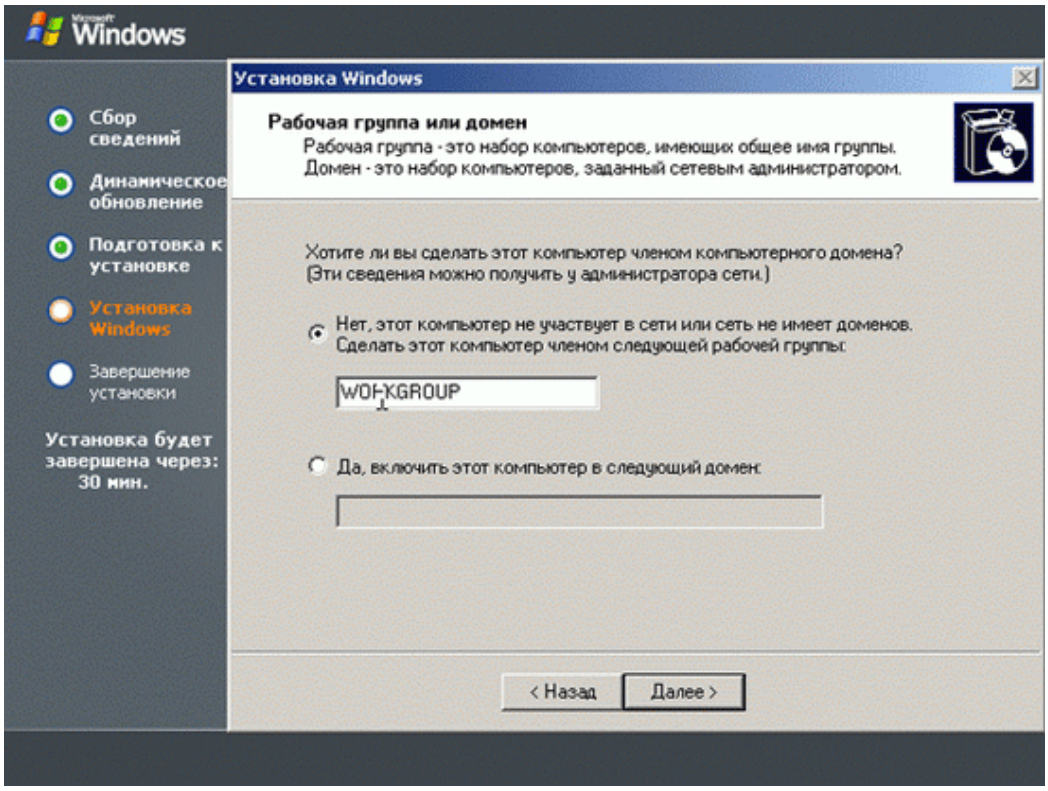


Рис. 25.

Дальнейшие действия по установке системы производятся автоматически. По окончании процесса установки необходимо нажать кнопку "Готово" и перезагрузить сервер.

5. Первоначальные действия по настройке сервера после установки операционной системы.

После перезагрузки сервера появится стандартное приглашение для входа в систему. Необходимо ввести имя пользователя "Администратор" и тот, пароль, который мы задали во время установки системы.

В настоящий момент сервер имеет имя DC1, входит в рабочую группу WORKGROUP, имеет начальные сетевые настройки, заданные во время установки. Теперь у нас имеется рабочий инструмент, который мы будем дополнять новыми компонентами и службами, менять его настройки и т.д. для изучения администрирования набора сетевых служб, который является базовым практически в любой корпоративной сети.

После первого входа в систему на экране появляется окно, представленное программой "Управление данным сервером" (рис. 2.26). Эта программа предназначена для управления ролями сервера, которые перечислены в начале данного раздела. Рекомендуем поставить галочку у поля "Не показывать эту страницу при входе в систему", т.к. ее показ при каждом входе будет мешать, а при желании снова эту программу запустить, ее ярлычок легко найти в разделе "Администрирование" главного меню.

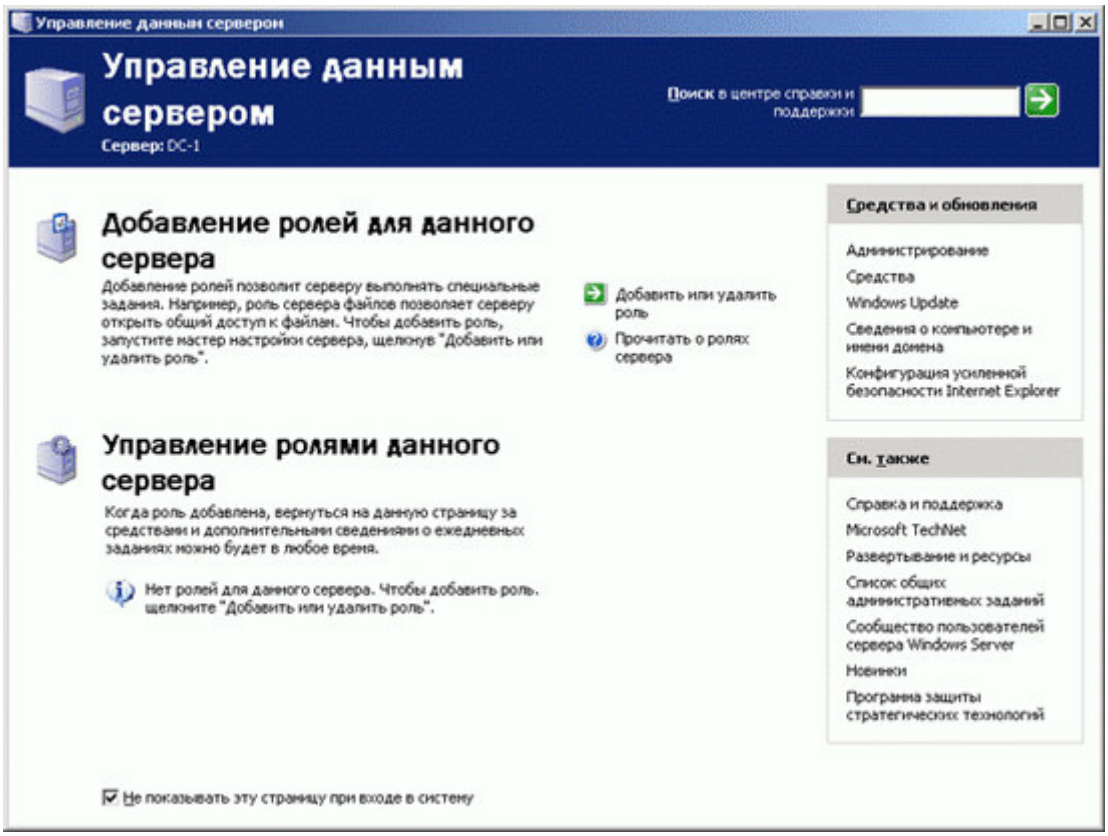


Рис. 26.

Кроме отключения постоянного вывода данного окна, при первом входе в систему можно настроить некоторые параметры рабочей среды администратора:

- параметры рабочего стола;
- параметры главного меню;
- разрешение экрана;
- способ просмотра папок (настоятельно рекомендуем, чтобы система показывала администратору все папки, в том числе системные и скрытые, а также включить показ расширений всех типов файлов).

6. Замечания по автоматической установке операционной системы Windows Server.

Вопросы автоматической установки системы не входят в данный учебный курс. Для получения начальной информации по этой теме рекомендуем ознакомиться с материалами, имеющимися на установочном компакт-диске. На этом CD есть папка\SUPPORT\TOOLS, в которой среди прочих имеется файл DEPLOY.CAB. В данном файле содержится ряд утилит, которые помогают автоматизировать процедуру установки системы и подготовить сценарии для тиражирования установки на большое количество серверов. Это в первую очередь программа установки winnt32.exe (и ее 16-битный собрат winnt.exe), которая в комбинации с различными ключами и параметрами может намного ускорить процесс установки. А также программыsetupmgr.exe и sysprep.exe. В файле DEPLOY.CAB имеется также файл deploy.chm, в котором содержится подробное описание использование всех данных утилит.

С дистрибутивного компакт-диска можно установить комплект ресурсов Windows Server 2003 Support Tools. Средства поддержки — это универсальный набор утилит для выполнения любых сервисных задач от диагностики системы до сетевого мониторинга.

Есть много способов администрирования систем Windows Server 2003. Чаще всего применяются следующие.

- Панель управления — набор средств для управления конфигурацией системы Windows Server 2003. В классическом меню Пуск (Start) доступ к этим средствам открывает подменю Настройка (Settings), в упрощенном меню Пуск (Start) команда Панель управления (Control Panel) доступна сразу.
- Графические средства администрирования — ключевые средства для управления компьютерами в сети и их ресурсами. Доступ к необходимому средству можно получить, щелкнув его значок в подменю Администрирование (Administrative Tools).
- Мастера администрирования — средства автоматизации ключевых административных задач. В отличие от Windows NT мастера не сосредоточены в

центральном месте — доступ к ним происходит посредством выбора соответствующих параметров меню и других средств администрирования.

- Функции командной строки. Большинство административных действий можно выполнять из командной строки.

В следующих разделах будут описаны эти функции администрирования.

Резюме

Операционные системы семейства *Windows Server* являются очень хорошим инструментом для изучения курса "Сетевое*администрирование*". Данные системы содержат богатый набор сетевых служб для изучения и практического освоения (при этом не потребуется приобретение специализированного дорогостоящего сетевого оборудования, достаточно иметь стандартный компьютерный *класс*, удовлетворяющий минимальным требованиям для установки системы):

- служба каталогов;
- службы сетевой инфраструктуры (DNS, DHCP, WINS);
- служба файлов и печати;
- сервер приложений (веб, электронная почта);
- службы терминалов;
- служба удаленного доступа/сервер виртуальной частной сети (VPN);
- сервер потокового мультимедиа-вещания.

Системы семейства *Windows Server* выпускаются в нескольких редакциях, каждая из которых содержит специфический для данной редакции набор сетевых служб и предъявляет свои требования к аппаратной конфигурации сервера, на котором данная система будет работать.

Планирование приобретения и установки системы в корпоративной сети требует рассмотрения и анализа широкого круга вопросов:

- определение набора ролей, которые будет выполнять данный сервер;
- расчет предполагаемой нагрузки на сервер (количество пользователей, объем обрабатываемой и передаваемой по сети информации);
- определение типа и количества процессоров и объема оперативной памяти;
- планирование дисковой подсистемы.

Процесс установки системы на сервере также требует предварительного планирования. Необходимо учесть такие параметры:

- способ установки (ручная или автоматическая);
- размещение дистрибутива системы (загрузочный CD, жесткий диск сервера, сетевая папка);

- будет ли система единственной на данном сервере или планируется использовать мультизагрузку различных экземпляров систем, установленных на различных дисках или различных разделах дисков;
- установка на "чистом" сервере или модернизация установленной ранее системы.

Самостоятельная работа

Упражнение 1. Установка операционной системы Windows 2003 Server (редакция Standard или Enterprise)

Цель упражнения	Освоить технологию ручной установки операционной системы Windows 2003 Server
Исходная конфигурация компьютера	Компьютер без операционной системы или с установленной системой Windows на разделе C:
Результат	Компьютер с установленной системой Windows 2003 Server
Предварительные навыки	Практические навыки работы в системе Windows

Задания

1 Установка системы

1. **Запуск установки**

Вариант 1

Вставить в CD-дисковод установочный CD

Загрузить компьютер с компакт-диска

Выбрать нужную редакцию системы

Вариант 2

Вставить в CD-дисковод установочный CD

Автоматически загружается программа установки системы

Выбрать пункт "Установить систему"

Вариант 3

Кнопка *"Пуск" — "Выполнить" — "Обзор"*

Найти открыть папку i386 на дистрибутиве операционной системы

Найти файл с именем winnt32.exe, запустить данный файл

2. **Процесс установки**

Текстовый режим

1. Выбор действий

"Чтобы приступить к установке Windows" нажмите *"Ввод*

2. Лицензионное соглашение

Нажмите клавишу *F8 - "Принимаю лицензионное соглашение"*

3. Разметка жесткого диска и выбор раздела для установки

Пример:

Неразмеченная область — 14345 МБ

С — *Создать раздел* (или выбрать существующий)

Создать раздел размером *5000 МБ*

Ввод — *"Установить"*

Выбрать

Форматировать раздел в системе *FAT/NTFS (Быстрое)*

4. Процесс копирования файлов
5. Перезагрузка компьютера

Графический режим

6. Определение устройств
7. Язык и региональные стандарты

Язык ввода по умолчанию — Русский

8. Настройка принадлежности программ

Введите значения текстовых полей (см. п. 3.2.):

Имя:

Организация.

9. Ключ продукта

Введите ключ для установки системы

10. Режим лицензирования

Задайте значение:

"На сервер" — 50

11. Имя компьютера и пароль администратора

Введите имя компьютера и пароль администратора сервера (см. п. 3.4-3.5.)

Пример (для варианта самостоятельного изучения)

Имя —DC 1

Пароль — *"пароль"*

12. Настройка времени и даты

Установите нужную дату и время

13. Установка поддержки сети
14. Сетевые параметры

Установите параметры протокола TCP/IP компьютера (см. п. 3.3.)

Выберите:

"Особые параметры"

Свойства TCP/IP — задайте параметры протокола TCP/IP

15. Рабочая группа или домен

Оставьте по умолчанию рабочую группу WORKGROUP

16. Снова процесс копирования файлов
17. Завершающие действия по установке системы (настройка Главного меню, регистрация компонентов, сохранение настроек и т.д.)

Специфические моменты

0. *Драйверы устройств*

В процессе установки могут потребоваться драйверы для устройств, для которых в БД драйверов системы нет соответствующего драйвера.

Если вы занимаетесь в группе под руководством преподавателя, то он предоставит все необходимые драйверы.

Если вы занимаетесь индивидуально, то сами позаботьтесь о необходимых драйверах для ваших компьютеров.

1. *Ввод сведений о пользователе*

В полях *"Пользователь"* и *"Организация"* введите любую текстовую информацию (например, Userv\ Company)

2. *Настройка сетевых подключений*

Протокол TCP/IP

Значение IP-адреса и маски подсети необходимо взять из таблицы распределения IP-адресов и имен компьютеров — введите параметры того компьютера, который назначен для вас преподавателем; значения остальных параметров протокола TCP/IP оставьте пустыми

3. *Выбор имени компьютера*

Выберите имя компьютера из таблицы распределения IP-адресов и имен компьютеров — введите то имя, которое назначено для вас преподавателем

4. *Пароль администратора*

Если вы занимаетесь в группе под руководством преподавателя, то он даст необходимые рекомендации (в большинстве случает можно оставить пустой пароль).

Если вы занимаетесь индивидуально, то назначьте пароль администратора таким образом, чтобы защитить вашу учебную конфигурацию от несанкционированного доступа и повреждения информации.

Завершение установки

0. *Выбор системы, загружаемой по умолчанию*

По окончании установки системы, после последней перезагрузки компьютера в момент появления меню выбора операционной системы выбрать ту систему, которая только что была установлена (данная установка должна выбираться по умолчанию).

1. *Региональные настройки*

Завершить настройку региональных параметров

2. *Настройка стандартного профиля пользователя*

Зарегистрируйтесь в системе с учетной записью администратора компьютера.

Настройте следующие параметры профиля:

- вид рабочего стола
- просмотр папок:
- показ полного пути в заголовке окна и строке адреса
- показ скрытых файлов и папок
- показ содержимого системных папок
- показ защищенных системных файлов
- показ расширений файлов
- показ сжатых и зашифрованных файлов другим цветом
- отмена запоминания вида каждой отдельной папки
- применить данный способ просмотр для всех папок
- свойства кнопки "Пуск" и "Главного меню" программ

Сделайте профиль администратора профилем по умолчанию

Если в процессе установки возникли те или иные вопросы, обсудите их с преподавателем в классе или в онлайн-форуме.

2.15 Лабораторная работа № 22, 23 (4 часа)

Тема: «Технология TokenRing»

2.15.1 Цель работы: изучить базовую технологию локальных сетей Token Ring, маркерный метод доступа к разделяемой среде.

2.15.2 Задачи работы:

1. Изучить технологию Token Ring;
2. Ознакомиться с маркерным методом доступа к разделяемой среде;
3. Рассмотреть физический уровень технологии Token Ring.

2.15.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.15.4 Описание (ход) работы:

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

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

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

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры - посланный кадр всегда возвращается в станцию - отправитель. В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

Для контроля сети одна из станций выполняет роль так называемого *активного монитора*. Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC-адреса, Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Чтобы сеть могла обнаружить отказ активного монитора, последний в работоспособном состоянии каждые 3 секунды генерирует специальный кадр своего присутствия. Если этот кадр не появляется в сети более 7 секунд, то остальные станции сети начинают процедуру выборов нового активного монитора.

Маркерный метод доступа к разделяемой среде

В сетях с *маркерным методом доступа* (а к ним, кроме сетей Token Ring, относятся сети FDDI) право на доступ к среде передается циклически от станции к станции по логическому кольцу.

В сети Token Ring кольцо образуется отрезками кабеля, соединяющими соседние станции. Таким образом, каждая станция связана со своей предшествующей и последующей станцией и может непосредственно обмениваться данными только с ними. Для обеспечения

доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения - маркер. В сети Token Ring любая станция всегда непосредственно получает данные только от одной станции - той, которая является предыдущей в кольце. Такая станция называется *ближайшим активным соседом, расположенным выше по потоку* (данных) - *Nearest Active Upstream Neighbor, NAUN*. Передачу же данных станция всегда осуществляет своему ближайшему соседу вниз по потоку данных.

Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца, что дает ей право доступа к физической среде и передачи своих данных. Затем эта станция выдает в кольцо кадр данных установленного формата последовательно по битам. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой. Кадр снабжен адресом назначения и адресом источника.

Все станции кольца ретранслируют кадр побитно, как повторители. Если кадр проходит через станцию назначения, то, распознав свой адрес, эта станция копирует кадр в свой внутренний буфер и вставляет в кадр признак подтверждения приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и передает в сеть новый маркер для обеспечения возможности другим станциям сети передавать данные. Такой алгоритм доступа применяется в сетях Token Ring со скоростью работы 4 Мбит/с, описанных в стандарте 802.5.

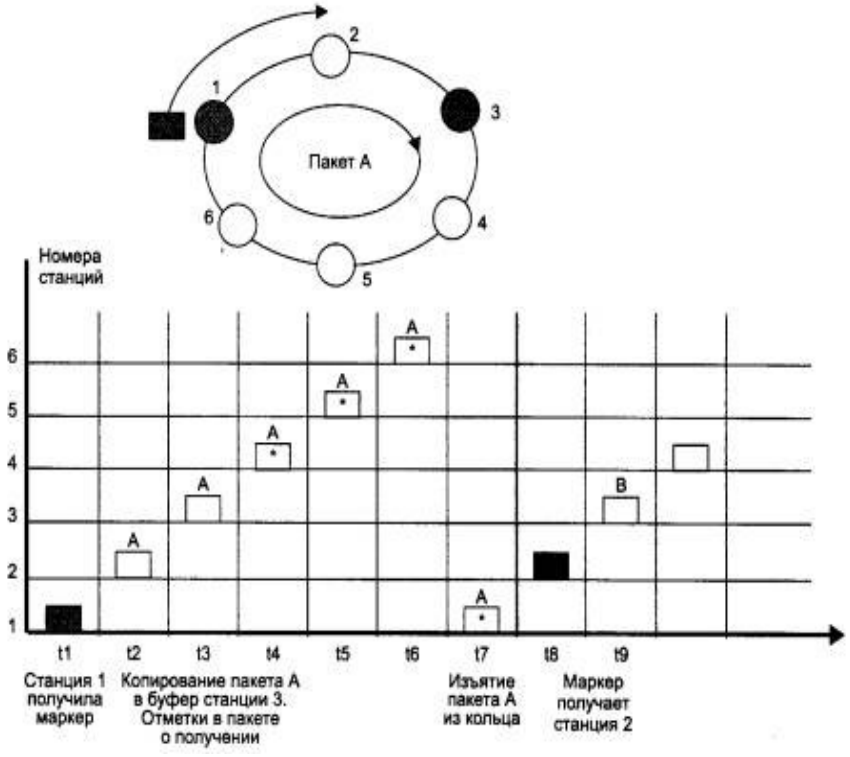


Рисунок 1 – Принцип маркерного доступа

На рисунке 1 описанный алгоритм доступа к среде иллюстрируется временной диаграммой. Здесь показана передача пакета А в кольце, состоящем из 6 станций, от станции *1* к станции *3*. После прохождения станции назначения *3* в пакете А устанавливаются два признака - признак распознавания адреса и признак копирования пакета в буфер (что на рисунке отмечено звездочкой внутри пакета). После возвращения пакета в станцию *1*отправитель распознает свой пакет по адресу источника и удаляет пакет из кольца. Установленные станцией *3* признаки говорят станции-отправителю о том, что пакет дошел до адресата и был успешно скопирован им в свой буфер.

Время владения разделяемой средой в сети Token Ring ограничивается *временем удержания маркера*, после истечения которого станция обязана прекратить передачу собственных данных (текущий кадр разрешается завершить) и передать маркер далее по кольцу. Станция может успеть передать за время удержания маркера один или несколько кадров в зависимости от размера кадров и величины времени удержания маркера. Обычно время удержания маркера по умолчанию равно 10 мс.

Для различных видов сообщений передаваемым кадрам могут назначаться различные *приоритеты*: от 0 (низший) до 7 (высший). Решение о приоритете конкретного кадра принимает передающая станция. Маркер также всегда имеет некоторый уровень текущего приоритета. Станция имеет право захватить переданный ей маркер только в том случае, если приоритет кадра, который она хочет передать, выше (или равен) приоритета маркера. В противном случае станция обязана передать маркер следующей по кольцу станции.

За наличие в сети маркера, причем единственной его копии, отвечает активный монитор. Если активный монитор не получает маркер в течение длительного времени (например, 2,6 с), то он порождает новый маркер.

Физический уровень технологии Token Ring

Стандарт Token Ring фирмы IBM изначально предусматривал построение связей в сети с помощью концентраторов, называемых MAU (Multistation Access Unit) или MSAU (Multi-Station Access Unit), то есть устройствами многостанционного доступа (рисунок 6.3). Сеть Token Ring может включать до 260 узлов.

Концентратор Token Ring может быть активным или пассивным. Пассивный концентратор просто соединяет порты внутренними связями так, чтобы станции, подключаемые к этим портам, образовали кольцо. Такое устройство можно считать простым кроссовым блоком за одним исключением - MSAU обеспечивает обход какого-либо порта, когда присоединенный к этому порту компьютер выключают. Такая функция необходима для обеспечения связности кольца вне зависимости от состояния подключенных компьютеров.

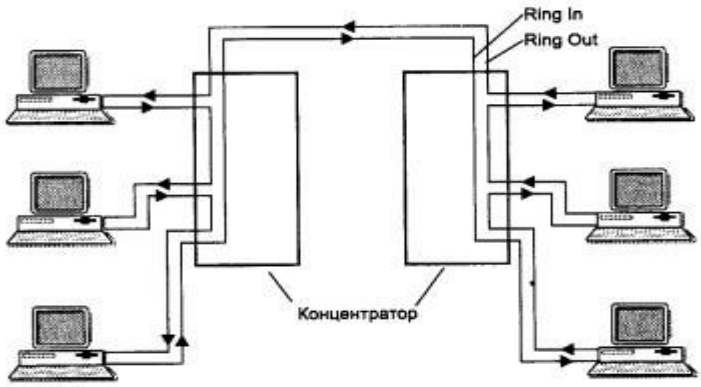


Рисунок 2 – Физическая конфигурация сети Token Ring

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

Возникает вопрос – если концентратор является пассивным устройством, то каким образом обеспечивается качественная передача сигналов на большие расстояния, которые возникают при включении в сеть нескольких сот компьютеров? Ответ состоит в том, что роль усилителя сигналов в этом случае берет на себя каждый сетевой адаптер, а роль ресинхронизирующего блока выполняет сетевой адаптер активного монитора кольца. Каждый сетевой адаптер Token Ring имеет блок повторения, который умеет регенерировать и ресинхронизировать сигналы, однако последнюю функцию выполняет в кольце только блок повторения активного монитора.

Максимальная длина кольца Token Ring составляет 4000 м. Ограничения на максимальную длину кольца и количество станций в кольце в технологии Token Ring не являются такими жесткими, как в технологии Ethernet. Здесь эти ограничения во многом связаны со временем оборота маркера по кольцу (но не только – есть и другие соображения, диктующие выбор ограничений). Так, если кольцо состоит из 260 станций, то при времени удержания маркера в 10 мс маркер вернется в активный монитор в худшем случае через 2,6 с, а это время как раз составляет тайм-аут контроля оборота маркера.

Контрольные вопросы

1) Что подразумевается под термином “Token Ring”.
2) Объясните технологию Token Ring.
3) Сравните технологии Ethernet и Token Ring.

2.16 Лабораторная работа № 24 (2 часа)

Тема: «Технология FrameRelay»

2.16.1 Цель работы: Архитектура и технологии построения сетей на базе протоколов X.25 и Frame Relay.

2.16.2 Задачи работы:

1. Изучить архитектуру построения сетей на базе протоколов X.25 и Frame Relay;
2. Ознакомиться с уровнями технологии Frame Relay.

2.16.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.16.4 Описание (ход) работы:

Для технологий построения глобальных сетей (WAN) характерно использование общей внешней физической среды в виде цифровых каналов передачи, связывающих попарно узлы коммутации между собой и с абонентскими системами (по принципу «точка – точка»).

В качестве физической среды для глобальных ТКС могут использоваться цифровые каналы существующих магистральных и зоновых первичных сетей, а также сетей телефонных абонентских линий с дополнительным использованием при необходимости специальных модемов, способных образовывать цифровые каналы на основе каналов ТЧ, ШК или просто через имеющуюся проводную или беспроводную среду передачи. Кроме того, в качестве внешней физической среды для одних глобальных ТКС могут выступать другие глобальные и локальные сети, исполняющие роль транспортных сетей или сетей абонентского доступа.

Архитектура и технологии построения сетей X.25

X.25 – это технология построения сети передачи данных с коммутацией пакетов. Архитектура X.25 включает описание процедур (протоколов) трех нижних уровней ЭМВОС: физического, звена данных и сетевого (а также частично транспортного). Сети X.25 отличаются способностью работать по каналам низкого качества с вероятностью ошибки в канале передачи до 0,01, но, как правило, с небольшой скоростью (единицы – десятки килобит в секунду). Основной недостаток – невозможность интерактивной работы в режиме реального времени (время доставки пакетов является случайным и относительно большим).

Более точно Рекомендация (стандарт, технология) X.25 имеет следующее название: «Интерфейс между оконечным оборудованием данных (ООД или DTE – Data Terminal Equipment) и аппаратурой окончания канала данных (АКД или DCE – Data Channel Equipment) для оконечных установок, работающих в пакетном режиме и подключенных к сетям передачи данных общего пользования по выделенному каналу».

Функционально границу между ООД и АКД можно провести между физическим уровнем оконечного устройства, реализующего полный стек протоколов X.25, и физической средой в виде входа/выхода цифрового канала (в частности, модема), связывающей оконечное устройство с ближайшим ЦКП. Иногда эту границу изображают между физическим уровнем и уровнем звена данных, что не совсем корректно.

В целом под АКД чаще всего понимается модем, иногда оконечное устройство (стартстопный терминал), которое не полностью реализует все функциональные возможности X.25 и подключается к сети через PAD.

PAD используется для доступа в сеть терминалов при асинхронном режиме обмена информацией (посимвольном). PAD обычно имеет несколько асинхронных портов и один синхронный порт X.25. PAD накапливает поступающие через асинхронные порты данные, упаковывает их в пакеты и передает через порт X.25.

Компьютеры и локальные сети обычно подключаются к сети X.25 непосредственно через адаптер X.25 или маршрутизатор, поддерживающий на своих интерфейсах протоколы X.25. В настоящее время устройства PAD используются в основном для подключения к сетям X.25 кассовых терминалов и банкоматов, имеющих асинхронный интерфейс RS-232(V.24/V.28). Для увеличения расстояния между терминалами и PAD от единиц – десятков метров до нескольких километров может использоваться интерфейс «токовая петля», а в случае еще большего удаления – модемы для работы по различным доступным каналам передачи, в частности, по выделенным или коммутируемым каналам ТЧ ТФОП.

Для соединения разных сетей X.25 посредством интерфейса X.75 могут использоваться специальные устройства – сигнальные терминальные коммутаторы пакетов (СТКП).

Архитектура сети X.25 в отличие от других сетей вполне соответствует концепции ЭМВОС в части, касающейся трех нижних уровней, и относительно хорошо сопрягается с протоколами OSI более высоких уровней.

Физический уровень. Стыки между ООД и АКД содержат: механические характеристики; электрические характеристики;

функциональные характеристики, задающие тип, число и назначение соединительных цепей стыка ООД/АКД;

процедурные характеристики, определяющие последовательность изменения состояния цепей интерфейса ООД/АКД, т. е. логику взаимодействия на физическом уровне.

Уровень звена данных. В Рекомендации X.25/2 указывается на необходимость использования на уровне звена данных процедуры управления звеном***LAPB*** (*Link Access Protocol, Balanced*). Процедура является сбалансированной (симметричной), т. е. как ООД, так и АКД могут инициировать начало обмена данными.

Поле «***Флаг***» разграничивает окончание предыдущего кадра и начало следующего (в отличие от кадров LLC, в которых для выделения границ используется преамбула на физическом уровне и указатель длины информационного поля на уровне MAC). Флаг имеет длинуWКС.фл = 1 байт и постоянное значение 01111110. Для исключения случайного совпадения комбинаций битов в информационном поле данных с флагом используется

процедурабит-стаффинга,в соответствии с которой передатчик, формирующий кадр, после каждой комбинации из пяти единиц вставляет бит «0», а приемник, обнаружив данную комбинацию, этот бит изымает.

Использование флагов позволяет не оговаривать заранее длину информационного поля данных*И*КИ, поэтому она может произвольно меняться в зависимости от размера ПБД сетевого уровня*И*С или качества используемой среды передачи (чем хуже качество, тем короче должны быть кадры, и наоборот). Как правило, при установлении соединения согласуется только максимальный размер информационного поля данных. В сетях X.25 он обычно не превышает максимальную длину пакетов 210 = 1024 байт.

Поле «***Адрес***» в составе кадра при двухточечном соединении на уровне звена данных X.25 в отличие от многоточечной среды передачи LAN в общем случае теряет смысл. Однако в формате кадра LAPB такое поле осталось, но значительно сокращенной длины*И*КС.адр = 1 байт (вместо 12 байт). При этом используется данное поле для идентификации команд и ответов. Команды от АКД к ООД и ответы на них имеют адреса 11000000, а команды от ООД к АКД и ответы на них имеют адреса 10000000. Кадры с другими адресами не рассматриваются и стираются как в ООД, так и в АКД.

Поле «***Управление***» кадры в нем могут быть трех типов: I – информационные; S – супервизорные и U – ненумерованные.

Поле «***Данные***» имеется только в информационныхI-кадрахи предназначено для передачи без изменений пакета сетевого уровня X.25, который обычно имеет длину*И*КИ = 2*n*, где*n* =4–10.

Поле «***Периодическая проверочная последовательность***» (CRC –*Cyclic Redundancy Code*), предназначено для обнаружения ошибок в кадре (без учета флагов), имеет длину *И*КС.обн.ош = 2 байта. Важной отличительной особенностью технологии X.25/2 (LAPB) является обязательный запрос повторения кадров, в которых после проверки поля CRC обнаруживаются ошибки. До подтверждения правильного приема очередного кадра уровень звена данных не будет принимать следующие кадры. Это является одной из причин случайных и длительных задержек передачи информации в сетях X.25.

Сетевой уровень. В соответствии с Рекомендацией X.25/3 протокол сетевого уровня (***PLP*** –*Packet Level Protocol*) предоставляет пользователю возможность информационного взаимодействия с другими пользователями сети посредством временных (***SVC*** – *Switch Virtual Circuit*) или постоянных (***PVC*** – *Permanent Virtual Circuit*) виртуальных каналов, а также путем обмена дейтаграммами. Режим обмена дейтаграммами не получил большого распространения, и в последних версиях стандарта он отсутствует. Наиболее распространены временные соединения (SVC), так как они обеспечивают лучшее использование

ограниченной пропускной способности глобальной сети при наличии большого количества пользователей.

В связи с тем, что в 1970-егг., когда появилась технология X.25, еще не существовала семиуровневая ЭМВОС и отсутствовало понятие транспортного уровня, ряд функций последнего фактически взял на себя сетевой уровень в дополнение к основным функциям, связанным с маршрутизацией.

Архитектура и технологии построения сетей Frame Relay

Frame Relay – это технология построения сети передачи данных с ретрансляцией кадров, являющейся разновидностью быстрой коммутацией пакетов. Технология была создана для замены технологии X.25 путем ее упрощения с целью повышения эффективности передачи данных по высокоскоростным и надежным цифровым каналам. Стандарты FR описывают интерфейс доступа к сетям с быстрой коммутацией пакетов и включают процедуры (протоколы) двух нижних уровней ЭМВОС – физического и звена данных (не полностью, но с дополнительными функциями сетевого уровня). Как и X.25, технология обеспечивает образование и поддержку множества независимых виртуальных каналов в одном звене, но не имеет средств коррекции и восстановления кадров при возникновении ошибок. Вместо средств управления потоком в протоколе FR реализованы функции извещения о перегрузках в сети. Могут использоваться также более длинные кадры, чем в протоколе X.25/2.

FR позволяет эффективно передавать крайне неравномерно распределенный во времени трафик. Отличается малым временем задержки, скоростями до 2 Мбит/с, эффективным использованием пропускной способности каналов передачи. В отличие от сетей X.25 позволяет обеспечивать интерактивный обмен оцифрованными речевыми сообщениями. Недостаток – требует каналы высокого качества (с вероятностью ошибки 10–7 и лучше).

Типовая структура и состав сети Frame Relay показаны на рис. 4. Основными элементами сети FR являются оконечные устройства (терминалы), устройства доступа к сетям с ретрансляцией кадров

FRAD (*FrameRelayAccessDevice*или по аналогии с PAD – *FrameRelayAssembler/Disassembler*– ассемблер/дизассемблер ретрансляции кадров) и узлы коммутации, а также связывающие их между собой каналы физической среды передачи. Узлы коммутации (ЦКП), правильнее было бы назвать центрами коммутации кадров, поскольку пакеты как ПБД сетевого уровня в сетях FR не используются.

Узлы коммутации FR, используемые для соединения локальных сетей, часто обозначают в виде мостов (*bridge*) или коммутаторов (*switch*).

Адаптер FR

Terminal Terminal Terminal

LAN

Terminal Terminal Terminal

Рис. 4. Типоваяструктураисоставсети Frame Relay

В роли оконечных устройств сетей FR выступают компьютеры и локальные сети, подключаемые к сети FR через адаптер FR, коммутатор или маршрутизатор, поддерживающий на своих интерфейсах протоколы FR.

Возможность передачи речи в сетях FR побудила развитие технологий ***VoFR*** (*Voice over Frame Relay* – голос поверх Frame Relay) и создание шлюзов с ТФОП.

FR на уровне звена данных используется процедура доступа к каналу для канальных групп врежиме кадров – протокол ***LAPF*** (*LinkAccessProcedureforFramemodebearerservices*). Поле «***Флаг***» служит для разграничения кадров таким же образом, как в кадре LAPB (X.25/2). Поле «***Заголовок***» может содержать от двух до четырех октетов (байт) и включает несколько элементов рассмотренных ниже.

CR (*Command*/*Response*) – бит «опрос/финал» («команда/ответ»). Зарезервирован для возможного применения в протоколах более высоких уровней ЭМВОС. Этот бит не используется протоколом FR и «прозрачен» дляаппаратно-программныхсредств сети FR.

EA (*Extended Address*) – бит расширения адреса. Используется для расширения заголовка на целое число дополнительных октетов с целью указания адреса, состоящего более чем из 10 бит. Если этот бит установлен в «0», то он называется EA0 и означает, что в следующем байте имеется продолжение поля адреса, а если этот бит равен 1, то он называется EA1 и индицирует окончание поля заголовка.

FECN (*Forward Explicit Congestion Notification*) – бит уведомления (сигнализации) приемника о явной перегрузке. Устанавливается в «1» для уведомления получателя кадра о том, что произошла перегрузка в направлении передачи данного кадра.

BECN (*Backward Explicit Congestion Notification*) – бит уведомления (сигнализации) источника о явной перегрузке. Устанавливается в «1» для уведомления источника сообщения о том, что произошла перегрузка в направлении, обратном направлению передачи кадра, содержащего этот бит.

DE (*Discard Eligibility*) – битразрешениясброса. Устанавливается в «1» в случае явной перегрузки и указывает на то, что данный кадр может быть уничтожен в первую очередь.

Поле «***Данные***» содержит информационные данные пользователя и состоит из целого числа октетов. Его максимальный размер определен стандартом FRF и составляет 1600 октетов, но возможны и другие максимальные размеры (вплоть до 212 = 4096 октетов).

Поле «***FCS***» – проверочная последовательность кадра. Используется для обнаружения возможных ошибок при передаче кадров, как поле CRC в кадре X.25/2 (LAPB), также состоит из двух октетов.

Основная процедура передачи кадров протокола FR состоит в том, что если кадр получен без искажений, он должен быть направлен далее по соответствующему маршруту (а если с искажениями, то он просто стирается).

В случае возникновения перегрузки в сети FR предусмотрено предупреждение источника и приемника, а также узлов коммутации вдоль маршрута следования пакетов начиная с узлов, соседствующих с узлом, на котором возникла перегрузка. Для сигнализации о перегрузке может использоваться специальный объединенный протокол управления каналом ***CLLM*** (*Consolidated Link Layer Management*), передача служебной информации в котором осуществляется в информационном поле кадров (см. рис. 6). Этот протокол применяется для оповещения источника, в направлении которого нет попутных кадров для использования BECN.

Получив предупреждение о перегрузке, соседние узлы коммутации могут снизить скорость передачи или изменить маршрут следования кадров. Не дожидаясь реакции на перегрузку со стороны соседних узлов, для разрешения проблем, связанных с перегрузкой сети FR, ее узлы могут отказываться от приема каких-либокадров вообще или только той части кадров, в заголовке которых бит DE = 1.

Особенностью технологии FR является отказ от коррекции обнаруженных в кадрах искажений. Протокол FR подразумевает, что конечные узлы будут обнаруживать и корректировать ошибки за счет работы протоколов транспортного или более высоких уровней.

Сеть Frame Relay является сетью с коммутацией кадров или сетью с ретрансляцией кадров, ориентированной на использование цифровых линий связи. Первоначально технология Frame Relay была стандартизирована как служба в сетях ISDN со скоростью передачи данных до 2 Мбит/с. В дальнейшем эта технология получила самостоятельное развитие. Frame Relay поддерживает физический и канальный уровни OSI. Технология Frame Relay использует для передачи данных технику виртуальных соединений (коммутируемых и постоянных).

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

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

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

Сети Frame Relay широко используется в корпоративных и территориальных сетях в качестве:

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

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

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

Рис. 1.

На рисунке представлена структурная схема сети Frame Relay, где изображены основные элементы:

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

Физический уровень Frame Relay

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

Канальный уровень Frame Relay

В сети Frame Relay используется два типа виртуальных каналов: постоянные (PVC) и коммутируемые виртуальные каналы. На канальном уровне поток данных структурируется на кадры, поле данных в кадре имеет переменную величину, но не более 4096 байт. Канальный уровень реализуется протоколом LAP-F. Протокол LAP-F имеет два режима работы: основной и управляющий. В основном режиме кадры передаются без преобразования и контроля.

В поле заголовка кадра имеется информация, которая используется для управления виртуальным соединением в процессе передачи данных. Виртуальному соединению присваивается определенный номер (DLCI). DLCI (Data Link Connection Identifier) - идентификатор соединения канала данных.

Каждый кадр канального уровня содержит номер логического соединения, который используется для маршрутизации и коммутации трафика. При этом контроль правильности передачи данных от отправителя получателю осуществляется на более высоком уровне модели OSI.

Коммутируемые виртуальные каналы используются для передачи импульсного трафика между двумя устройствами DTE. Постоянные виртуальные каналы применяются для постоянного обмена сообщениями между двумя устройствами DTE.

Процесс передачи данных через коммутируемые виртуальные каналы осуществляется следующим образом:

- установление вызова - образуется коммутируемый логический канал между двумя DTE;
- передача данных по установленному логическому каналу;
- режим ожидания, когда коммутируемая виртуальная цепь установлена, но обмен данными не происходит;
- завершение вызова - используется для завершения сеанса, осуществляется разрыв конкретного виртуального соединения.

Процесс передачи данных через предварительно установленные постоянные виртуальные каналы осуществляется следующим образом:

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

Достоинства сети Frame Relay:

- высокая надежность работы сети;
- обеспечивает передачу чувствительный к временным задержкам трафик (голос, видеоизображение).

Недостатки сети Frame Relay:

- высокая стоимость качественных каналов связи;
- не обеспечивается достоверность доставки кадров.

2.17 Лабораторная работа № 25 (2 часа)

Тема: «Технология SDH»

2.17.1 Цель работы: изучить технологию высокоскоростной передачи — синхронной цифровой иерархии (SDH).

2.17.2 Задачи работы:

1. Изучить технологию SDH.

2.17.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютерная ЛВС.

2.17.4Описание (ход) работы:

Технология SDH описывается в рекомендациях ITU-T (G.702, G.703, G.704, G.707, G.708, G.709, G.773, G.774, G.782, G.783, G.784, G.957, G.958, Q.811, Q.812), ETSI (ETS 300 147). Североамериканская синхронная цифровая иерархия подчиняется системе стандартов

SONET, разработанной ANSI (American National Standards Institute) - Американским национальным институтом стандартов.

Рассмотрим структуру сигналов SDH. Это синхронный транспортный модуль STM-N, где N определяется уровнем SDH. В настоящее время широко используются системы STM-1, STM-4, STM-16 и STM-64. Нетрудно заметить, что системы построены с кратностью 4. Таким образом, сформировалась следующая иерархия скоростей.

Синхронная цифровая иерархия

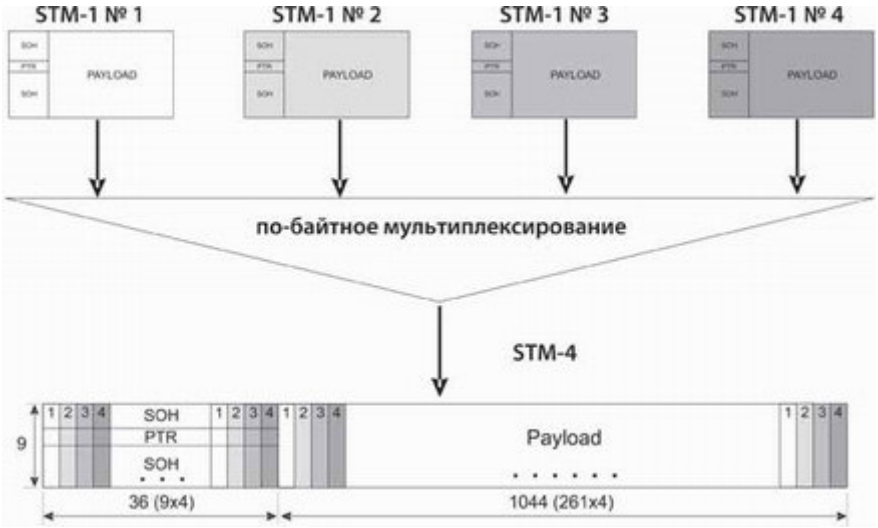
Уровень модуля	**Скорость (кбит/с)**
STM-1	155 520
STM-4	622 080
STM-16	2 488 320
STM-64	9 953 280

Базовым уровнем SDH является STM-1. Он характеризуется своим циклом с периодом повторения 125 мкс. Общепринято рассматривать цикл в виде прямоугольной таблицы, хотя, разумеется, данные передаются по линии последовательно. Как видно из рисунка цикл STM-1 содержит 9 строк по 270 байт (2430 байт). Первые 9 байт в каждой строке образуют заголовок цикла.

К преимуществам SDH следует отнести модульную структуру сигнала, когда скорость уплотненного сигнала получается путем умножения базовой скорости на целое число. При этом структура цикла не меняется и не требуется формирование нового цикла. Это позволяет выделять требуемые каналы из уплотненного сигнала без демультиплексирования всего сигнала.

На рисунке приводится схема мультиплексирования четырех потоков STM-1 в один поток STM-4. Из рисунка видно, что происходит по-байтное мультиплексирование таким образом,

что все блоки секционных заголовков, указатель и полезный сигнал размещаются так же как и прежде.



В качестве полезной нагрузки сети, построенной на основе SDH, могут передаваться сигналы PDH, ячейки ATM, любые неструктурированные цифровые потоки, имеющие скорость от 1,5 до 140 Мбит/с и удовлетворяющие рекомендации G.703. Такая универсальность обеспечивается применением контейнеров, переносящих по сети SDH сигналы нагрузки.

Контейнерный принцип хорошо известен и довольно широко применяется в современной технике связи. Эта идея оказалась очень практичной, ведь все операции на сети производятся с контейнерами и не затрагивают их содержимое. Таким образом, достигается полная прозрачность сети для передаваемой информации.

Формирование контейнеров для передачи данных с различной скоростью рассматривается ниже. Все контейнеры размещаются в части цикла STM-1, называемой Payload.

Во избежание потери синхронизации в аппаратуре SDH предусматривается скремблирование передаваемых сигналов. Дело в том, что в полезной информации могут присутствовать длинные цепочки нулей или единиц. При передаче по линиям электрических сигналов (например, в коаксиальном кабеле) эта проблема снимается выбором соответствующего кода линейного сигнала.

По рекомендации ITU-T G.703 следует применять код CMI (coded mark inversion code, двухуровневый код с инверсией посылок). В этом коде передаваемый ноль всегда представляется отрицательным уровнем в первой половине посылки и положительным уровнем во второй половине. Передаваемая единица представляется либо положительным уровнем, либо отрицательным уровнем в зависимости от значения предыдущего бита. В подавляющем большинстве случаев для передачи сигналов STM используются оптические

линии связи. В них используется линейный код NRZ (non return to zero, код без возврата к нулю).

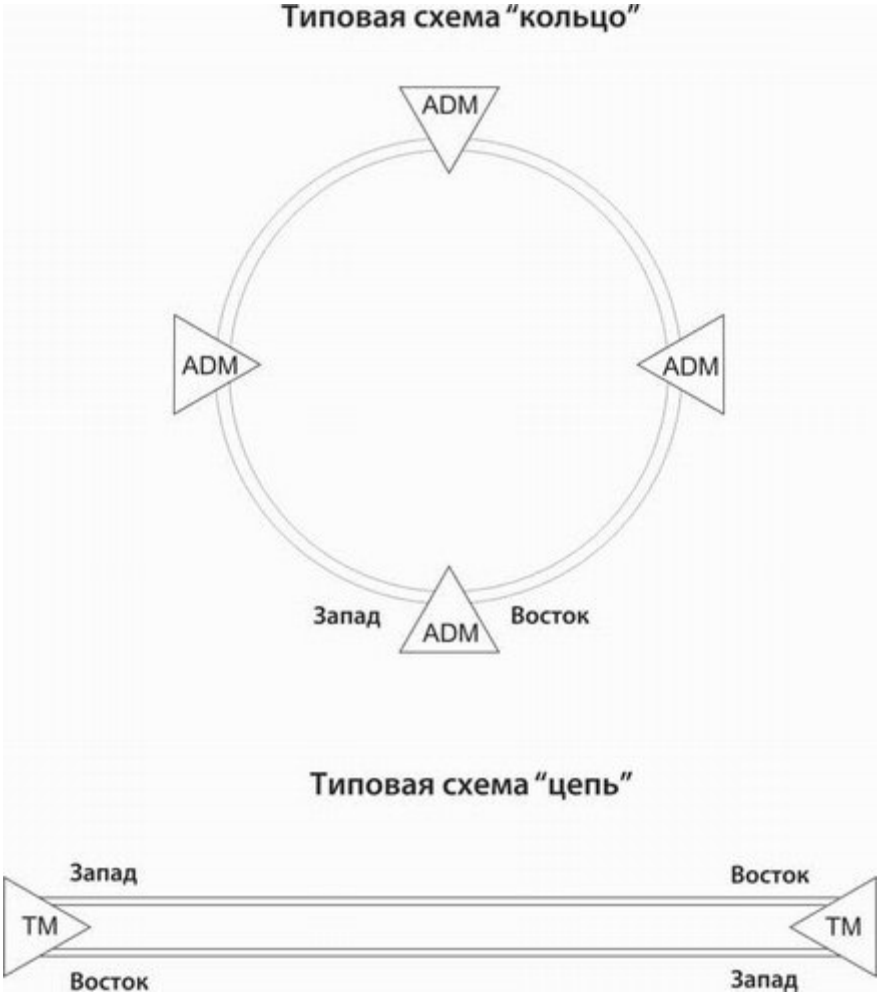
Именно для обеспечения хронирующих перепадов в передаваемом сигнале STM по оптическим линиям связи используется операция скремблирования. Скремблер преобразует исходный цифровой поток в псевдослучайную последовательность. Генератор псевдослучайной последовательности построен на основе семиразрядного сдвигового регистра, сумматоров по модулю 2 (“исключающее ИЛИ”) и обратных связей согласно полинома 1+X6+X7. Скремблированию подвергается весь цикл STM-N кроме первых 9 байт заголовка. В первой строке заголовка передается сигнал цикловой синхронизации, что позволяет осуществлять синхронизацию без предварительного дескремблирования.

Построение сети SDH любой сложности обеспечивается довольно ограниченным набором функциональных узлов. С помощью их выполняются все операции по передаче информации и управлению на сети. Основным функциональным узлом SDH является мультиплексор, предназначенный для организации ввода/вывода цифровых потоков с полезной нагрузкой. Различают два типа мультиплексоров: терминальные и ввода/вывода. Основное отличие между ними заключается в расположении на сети. Ниже, при рассмотрении типовых схем сетей SDH, это различие будет указано. Кросс-коннекторы обычно непосредственно не обслуживают ввод/вывод нагрузки, а обеспечивают обмен между транспортными модулями сети SDH. Кросс-коннекторы применяются при объединении сетей или при сложной топологии сети. Кроме специализированных кросс-коннекторов функции локальной коммутации может выполнять мультиплексор.

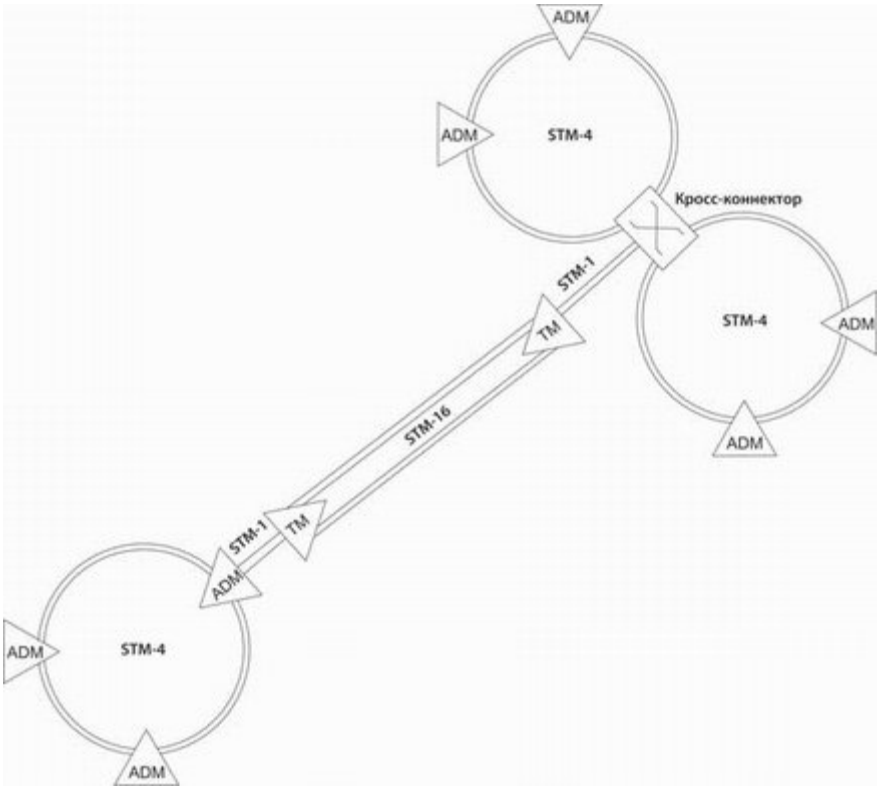
Ряд функциональных узлов, таких как регенераторы, оборудование линейных трактов и радиорелейных линий обеспечивают функционирование собственно линий передачи сети SDH.

Обязательным функциональным узлом любой серьезной сети SDH является система управления, с помощью которой обеспечивается мониторинг и управление всеми элементами сети и информационными трактами. В сетях SDH используются две типовых топологических схемы построения: “кольцо” и “цепь”. В их основе лежат мультиплексоры. В схеме “кольцо” применяются только мультиплексоры ввода/вывода (ADM -Add/Drop Multiplexer), а в схеме “цепь” - терминальные мультиплексоры (TM - terminal multiplexer) и ввода/вывода. Как видно из рисунка каждый мультиплексор имеет по две пары магистральных выходов, одна называется “восток”, а другая - “запад”. С помощью их обеспечиваются различные схемы резервирование или защиты. Схемы защиты типа “1:1” и типа “1+1” образуются за счет организации двух встречных потоков. В первом случае на приеме анализируются сигналы с каждого направления и выбирается лучший для дальнейшей обработки. Во второй схеме

существуют два кольца - основное и резервное. При сбоях в основном кольце происходит переключение на резервное, в случае разрыва кольца или выхода из строя мультиплексора образуется новое кольцо за счет организации заворотов на границах поврежденного участка.



Из рассмотренных типовых схем или их разновидностей можно создать сеть SDH любой архитектуры и любой сложности.



На рисунке представлена абстрактная сеть SDH, включающая в себя магистральный участок большой протяженности и подсети на концах этой магистрали. В городе Б существуют две сети кольцевой архитектуры, объединенные с помощью кросс-коннектора. Через него информационные потоки могут попадать в магистральную сеть, выполненную по схеме “цепь”. В городе А расположена одна сеть кольцевой архитектуры. Обмен данными с магистральной сетью осуществляется с помощью мультиплексора ввода/вывода (ADM). Из-за большой протяженности магистральной сети, при отсутствии потребности в промежуточных пунктах ввода/вывода данных, на ней используются регенераторы, обеспечивающие восстановление формы сигнала. Такая схема организации требуется очень редко. Предпочтительнее вместо регенераторов использовать мультиплексоры ввода/вывода, которые так же обеспечивают регенерацию цифрового сигнала.

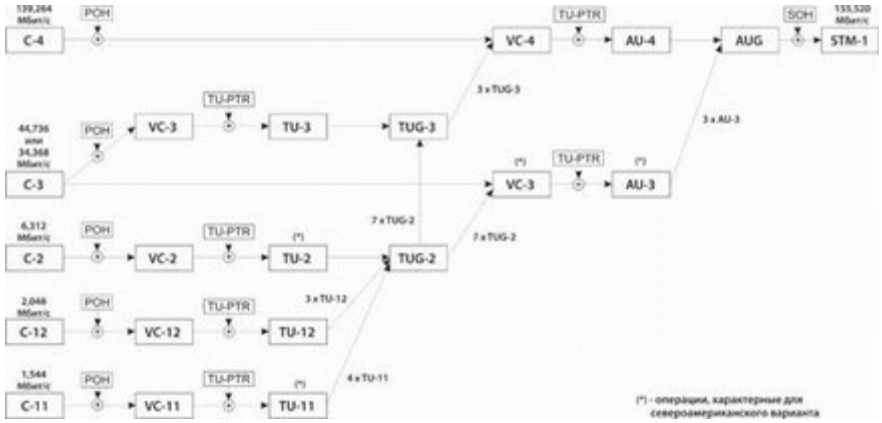
Участок сети между двумя терминальными мультиплексорами называют маршрутом. Между двумя соседними мультиплексорами (кросс-коннекторами) - мультиплексорной секцией, а между двумя соседними регенераторами или между регенератором и мультиплексоросм (кросс-коннектором) - регенерационной секцией.

Размещение данных в цикле STM-1 (mapping)

Как отмечалось выше, вся полезная информационная нагрузка (payload) передается при помощи контейнеров. Рассмотрим возможные типы контейнеров, их внутреннюю структуру и принципы формирования. Определено следующее соответствие контейнеров скоростям передачи полезной информации (в кбит/с):

Контейнер	Скорость передачи (кбит/с)
C11	1 544
C12	2 048
C2	6 312
C3	44 736 или 34368
C4	139 264

Этот ряд контейнеров соответствует международным рекомендациям (ITU-T G.709) и объединяет европейскую и североамериканскую схемы системы SDH (SONET). В европейский стандарт не входит контейнер C2.
На рисунке показана общая схема размещения сигналов в синхронной цифровой иерархии.



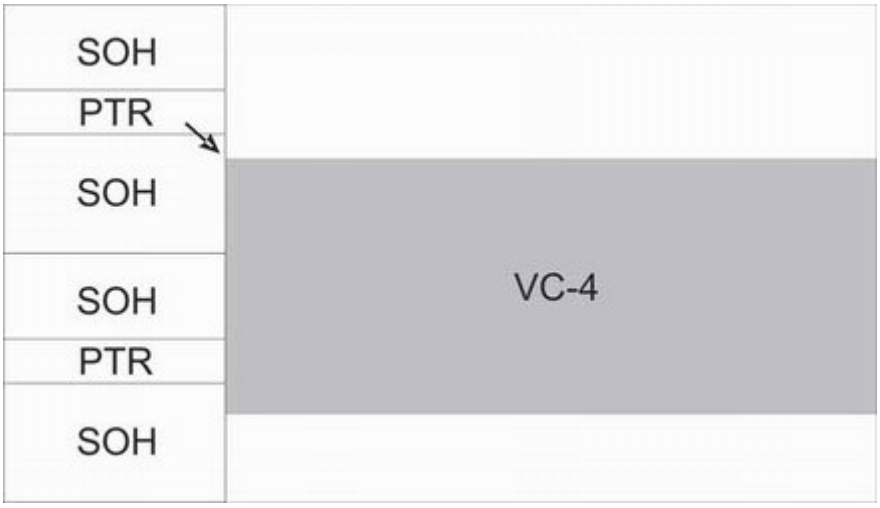
Сигнал PDH со скоростью 140 Мбит/с (139 264 кбит/с) при передаче через сеть SDH размещается в контейнерах C-4. Контейнеры C-4 следуют с периодом 125 мкс. Размер контейнера C-4 точно определен и составляет 2340 байт (9 строк по 260 байт) или 18720 бит. В то же время для размещения всех бит сигнала PDH со скоростью 140 Мбит/с требуется контейнер емкость всего 17408 бит (139 264 кбит/с : 8 кГц). Величина 8 кГц соответствует периоду повторения в 125 мкс. Таким образом, в контейнере C-4 остается еще место, которое не было заполнено сигналом PDH. Это пространство содержит:

- биты и байты грубого выравнивания (постоянный стаффинг) для согласования скорости плезиохронного сигнала с более высокой скоростью контейнера;
- биты точного выравнивания, используется положительный стаффинг (добавление бит);
- биты с информацией о наличии точного выравнивании;
- биты “балласта”, которые не имеют функционального назначения.

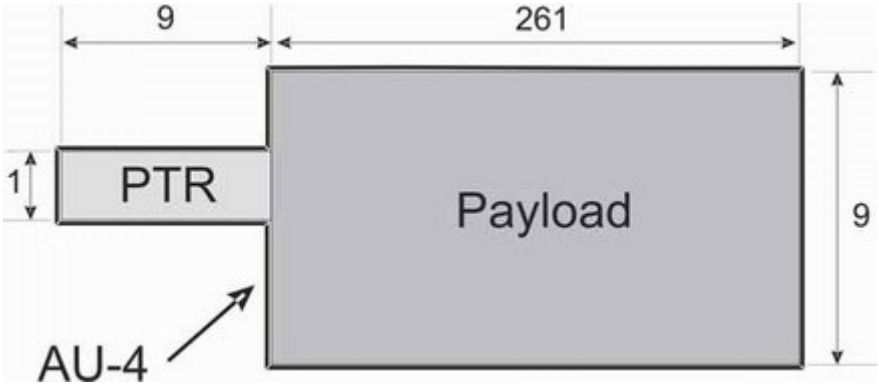
Для передачи в потоке STM-1 контейнера C-4 к нему добавляется путевой или трактовый заголовок POH (Path OverHead) размером 9 байт. В результате этой операции

образуется так называемый виртуальный контейнер VC-4, имеющий размер 2349 байт (9 строк по 261 байту).

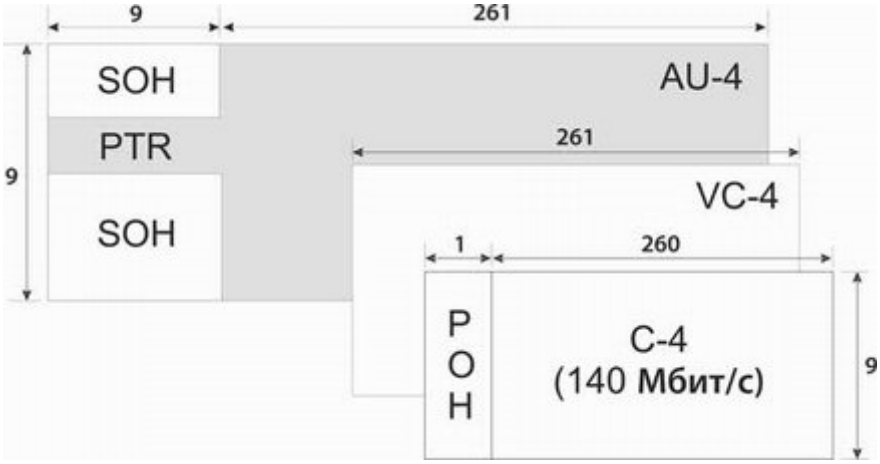
Поскольку циклы STM-1 формируются непрерывно и синхронно по отношению ко всей сети, то для обеспечения передачи плезиохронных сигналов используют гибкую укладку виртуальных контейнеров VC-4 в потоке STM-1. Как будет показано ниже начало VC-4 размещается в одном цикле STM-1, остаток в следующем цикле.



Информация о начале виртуального контейнера VC-4, расположении его первого байта содержится в указателе PTR (Pointer). Подробнее указатели рассматриваются ниже. В цикле STM-1 указатель PTR и Payload вместе называются административным блоком AU-4.

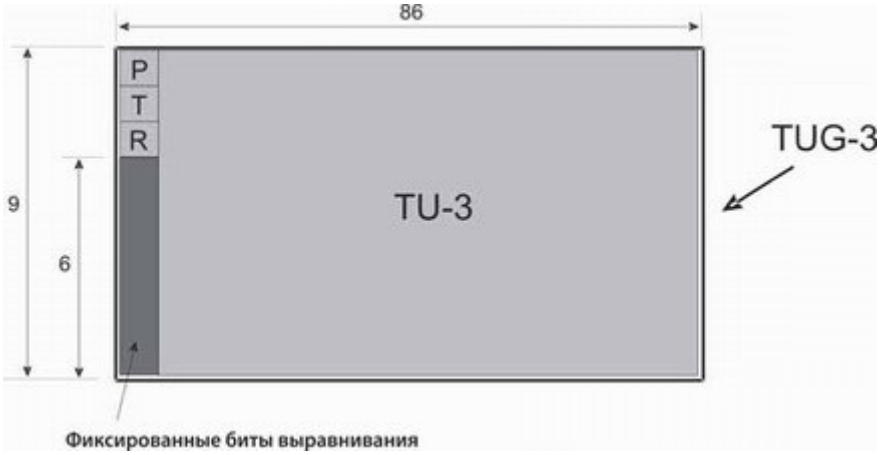


Указатель носит название AU-4 указатель (AU-4 PTR). Для получения полной структуры цикла STM-1 к блоку AU-4 добавляются секционные заголовки (SOH). На рисунке показана взаимосвязь между составляющими цикла STM-1 при размещении контейнера С-4.

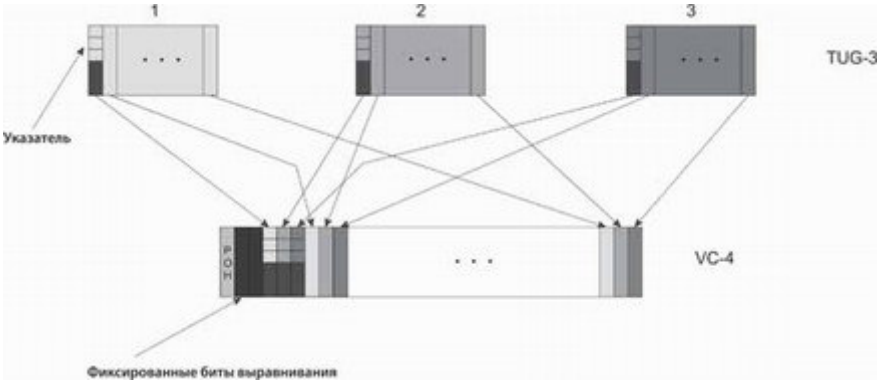


В цикле STM-1 может быть передано 3 контейнера сигналов PDH со скоростью 34 Мбит/с (34 368 кбит\с). Эти контейнеры носят название С-3. Если посмотреть с позиции скорости, то цикл STM-1 может передавать 4 сигнала со скоростью 34 Мбит/с, однако для совместимости с североамериканской системой SONET используется только 3 контейнера С-3.

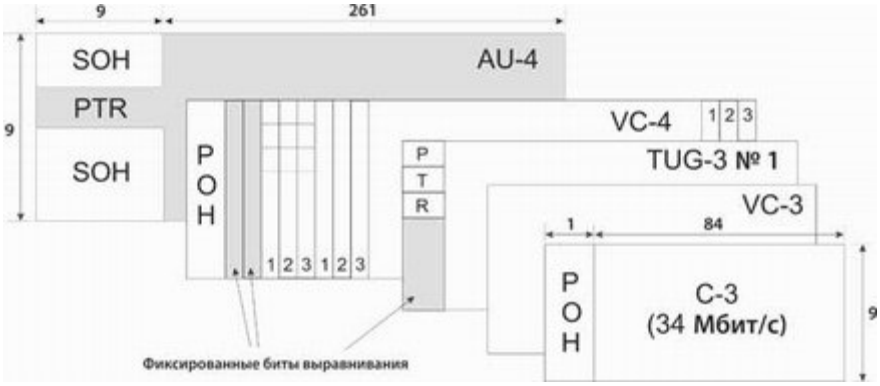
Контейнер С-3 имеет размер 756 байт (9 строк по 84 байта) или 6048 бит. Период следования контейнера С-3 - 125 мкс. Для передачи сигнала PDH со скоростью 34 Мбит/с требуется емкость контейнера всего 4296 бит (34 368 кбит/с : 8 кГц). Контейнер С-3 также предназначается для размещения сигнала DS-3 североамериканской иерархии (44 Мбит/с). Для этого в контейнере С-3 задействуется только 5593 бита (44 736 кбит/с : 8 кГц). Свободные биты, оставшиеся после размещения полезной нагрузки, используются так же как в контейнере С-4. Только для точного выравнивания используется двухсторонний стаффинг (добавление и вычитание бит). К каждому контейнеру С-3 добавляется заголовок POH и в результате получается виртуальный контейнер VC-3, имеющий размер 765 байт (9 строк по 85 байт). Существует два способа размещения контейнера VC-3 в цикле STM-1. При первом способе каждому виртуальному контейнеру VC-3 в цикле STM-1, точнее в его указателе PTR, соответствует отдельный 3-х байтный указатель. Совокупность контейнера VC-3 и 3-х байтного указателя образует административный блок AU-3. Указатель называется указатель AU-3 (AU-3 PTR) и показывает начало соответствующего VC-3 в цикле STM-1. В стандартах ETSI, описывающих SDH, этот способ не рекомендуется для применения. Второй способ основан на преобразовании трех блоков VC-3 в один блок VC-4. Для этого к виртуальному контейнеру VC-3 добавляется 3-х байтный указатель, получается трибутарный блок TU-3. При добавлении к нему 6 фиксированных выравнивающих байтов получается группа трибутарного блока TUG-3.



Для передачи по сети SDH, три полученных блока TUG-3 по-байтно мультиплексируются в виртуальный контейнер VC-4. На рисунке показан этот процесс.

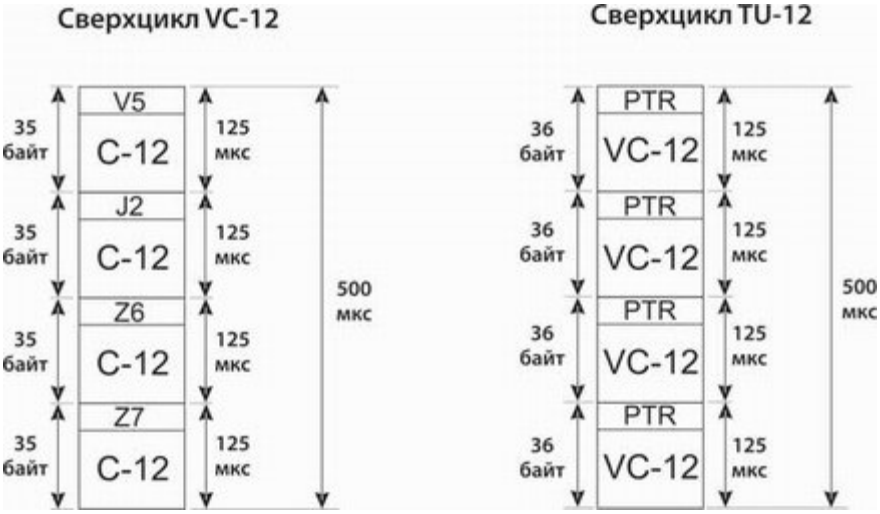


Заметим, что для согласования размеров контейнеров (и, следовательно, для согласования скоростей) в контейнере VC-4 после POH размещаются две колонки фиксированных байтов выравнивания. На рисунке приводится взаимосвязь между составляющими цикла STM-1 при размещении контейнеров C-3, согласно рекомендациям ETSI.

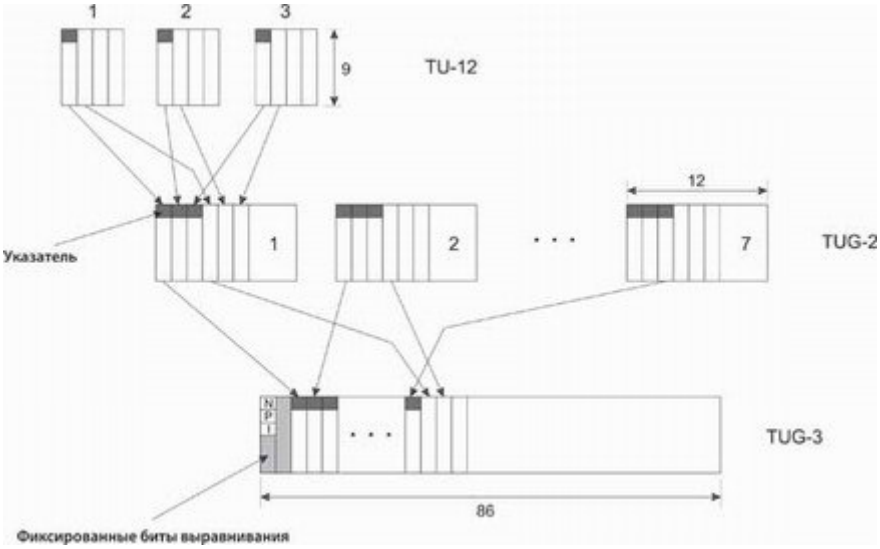


В цикле STM-1 может быть передано 63 контейнера сигналов PDH со скоростью 2 Мбит/с (2 048 кбит\с). Контейнер для передачи этого сигнала называется C-12. Период следования этого контейнера равен 125 мкс. Емкость контейнера 34 байта (8 строк по 4 байта плюс 1 строка в 2 байта) или 272 бита. Для передачи сигнала PDH 2 Мбит/с требуется 256 бит (2 048 кбит/с : 8 кГц). Свободные биты, оставшиеся после размещения полезной нагрузки, используются так же как

в контейнерах С-4 и С-3, применяется двухсторонний стаффинг для точного выравнивания. Виртуальный контейнер VC-12 образуется добавлением РОН размером в 1 байт в начало контейнера. При этом в 9 строке контейнера становится 3 байта, т.е. вся информация сдвигается назад на 1 байт.
Виртуальные контейнеры VC-12 передаются в составе сверхцикла (или мультифрейма), имеющего период в 500 мкс. Отметим, что сверхцикл передается за несколько циклов STM-1. Байты РОН каждого контейнера VC-12 одного сверхцикла составляют суммарный заголовок РОН. На рисунке показан составляющие сверхцикла. Значение байтов РОН (V5, J2, Z6 и Z7) будет пояснено при описании заголовка.



Трибутарный блок TU-12 образуется за счет добавления байта указателя к контейнеру VC-12. Размер TU-12 равен 36 байт (9 строк по 4 байта). Из сверхцикла контейнеров VC-12 образуется сверхцикл TU-12 путем добавления четырех байт указателя (TU-12 PTR). Значение имеют только первые три байта указателя, четвертый в настоящее время не имеет определенных функций. Подробнее данные указатели будут описаны ниже.
Три блока TU-12 путем по-байтного мультиплексирования образуют группу TUG-2 размером 108 байт (9 строк по 12 байт). Семь групп TUG-2 таким же образом объединяются в группу TUG-3 (рис. 5.13), при этом добавляется одина колонка фиксированных байтов выравнивания.



В полученной группе TUG-3 три байта, соответствующие указателю TU-3 PTR, называются NPI (Null Pointer Indicator) - индикатор “пустого” (не имеющего значения) указателя.

Из блоков TUG-3 формируется цикл STM-1 рассмотренным выше образом.

Указатели контейнеров (pointer)

Механизм указателей в SDH служит для синхронизации между различными трибутарными сигналами и циклом STM. Благодаря указателям не требуется взаимное согласование начала цикла SDH и цикла трибутарного сигнала, упакованного в виртуальный контейнер.

Указатели всегда размещаются на точно определенных местах в структуре сигнала SDH, благодаря чему возможен доступ к информации без демультиплексирования всего сигнала. Для выравнивания отклонений фазы и скорости передачи применяется двухсторонний стаффинг указателей. Всего имеется три типа указателей:

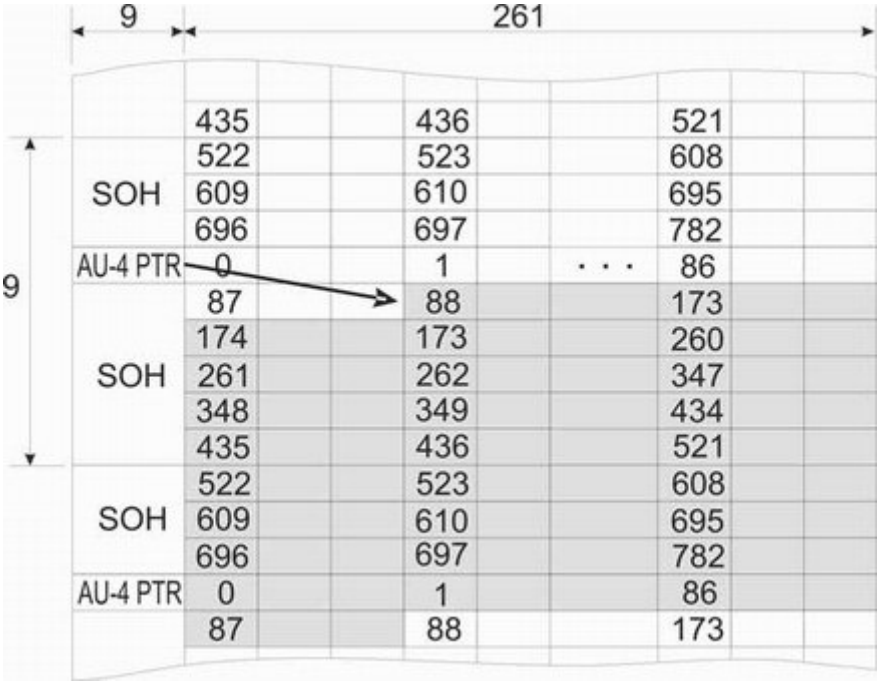
- указатели административного блока AU, AU-4 PTR и AU-3 PTR. Последний указатель применяется в североамериканской версии SDH и подробно рассматриваться не будет. Указатель AU-4 определяет размещение виртуального контейнера VC-4 в цикле STM-1;
- указатель трибутарного блока TU-3, TU-3 PTR. Данный тип указателя используется размещения трех виртуальных контейнеров VC-3 в виртуальном контейнере VC-4;
- указатели трибутарных блоков TU-11, TU-12 и TU-2. Эти указатели служат для размещения соответствующих виртуальных контейнеров VC-11, VC-12 и VC-2. Каждый их этих указателей передается по одному байту в трех первых циклах по 125 мкс в одном сверхцикле по 500 мкс. Байт на месте указателя в четвертом цикле сверхцикла не имеет значения и зарезервирован для будущих применений.

Байты указателей AU-4 PTR и TU-3 PTR содержат следующую информацию:

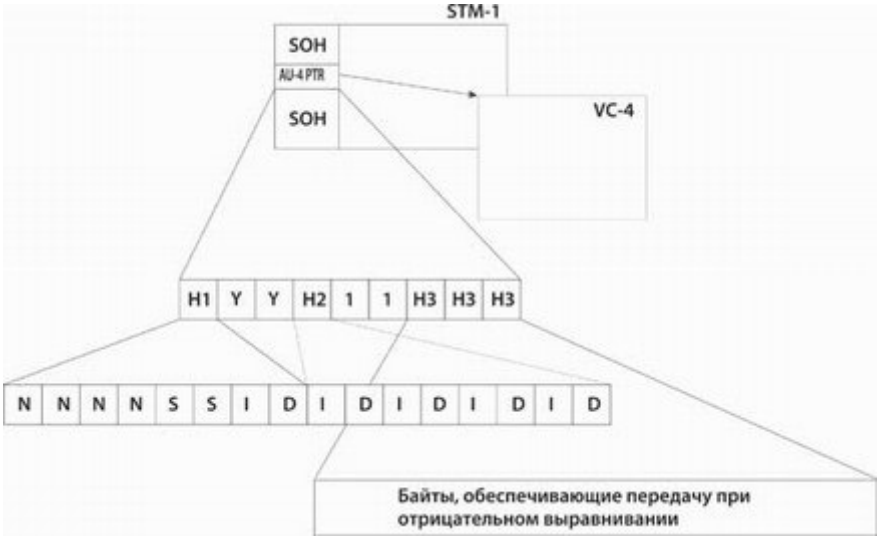
- адрес начала соответствующего виртуального контейнера;
- флаг новых данных;
- биты точного выравнивания;
- метка типа указателя (AU-4 PTR, AU-3 PTR или TU-3 PTR). В настоящее время эта метка не используется и должна иметь фиксированное значение;
- байты, применяющиеся при использовании отрицательного выравнивания.

Байты указателей TU-11 PTR, TU-12 PTR и TU-2 PTR содержат информацию об адресе начала соответствующего виртуального контейнера и поле для возможности отрицательного выравнивания.

Значения указателя AU-4 PRT позволяют адресоваться только к каждому третьему байту области payload цикла STM-1. Диапазон адресов в котором возможно “плавающее” начало контейнера VC-4 начинается следом за блоком AU-4 PTR с адреса 0 и заканчивается адресом 782 в следующем цикле STM-1. На рисунке показано начало виртуального контейнера MC-4 с адреса 88.



Ниже представлена структура указателя AU-4 PTR.



Байты H1 и H2 содержат следующие поля:

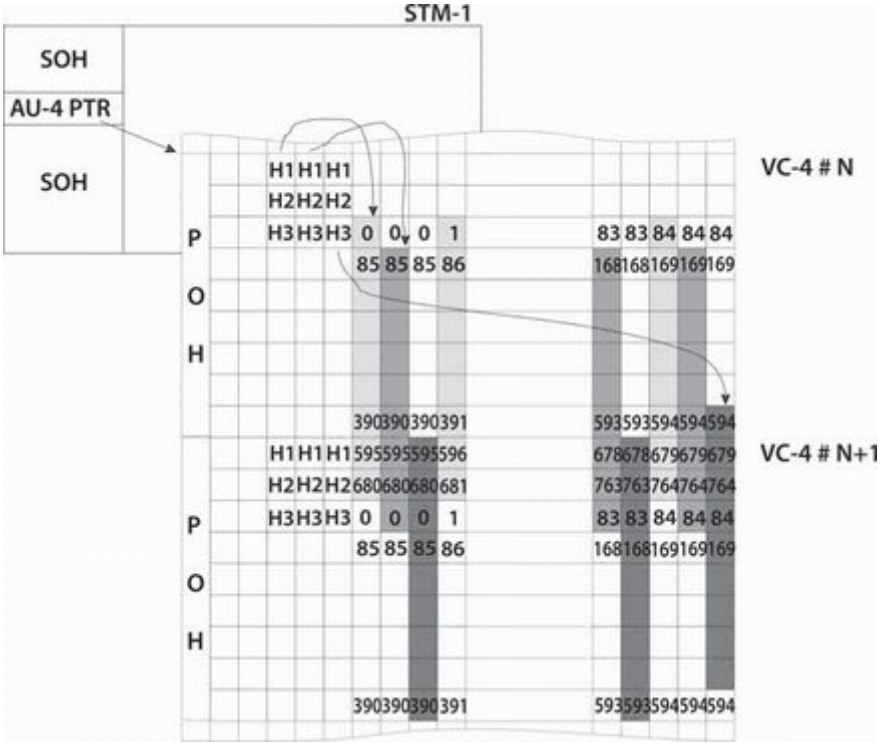
- поле флага новых данных, биты N. Данное поле может содержать два значения статуса “1001” и “0110”. Активный статус (“1001”) служит для уведомления приемника, что значение указателя было изменено. В последующих циклах и во время процедуры выравнивания используется неактивный статус (“0110”);
- поле метки типа указателя, биты S. В настоящее время не используются и должны иметь фиксированное значение “10”;
- поле значения указателя, 10 бит I и D. Эти биты имеют двойное назначение. Они могут определять значение указателя от 0 до 782 в десятичном исчислении. После передачи активного статуса в битах N значение указателя должно совпадать минимум в трех циклах. Для осуществления отрицательного выравнивания все D - биты инвертируются и в следующем AU-4 PTR значение указателя уменьшается на 1 (операция декремента). При положительном выравнивании инвертируются все I - биты и в следующем цикле осуществляется операция инкрементирования (значение указателя увеличивается на 1). Корректировка указателя допускается только один раз на четыре цикла для обеспечения подтверждения верности указателя.

Согласно рекомендациям ETSI байты “Y” и “1” не применяются и должны иметь постоянное значение. Байт “Y” содержит 1001SS11, где SS совпадают с полем метки типа указателя и имеют их же значение. Таким образом байт “Y” = “10011011”. Байт “1” всегда содержит “11111111”. В североамериканском варианте эти байты могут использоваться как дополнительные указатели.

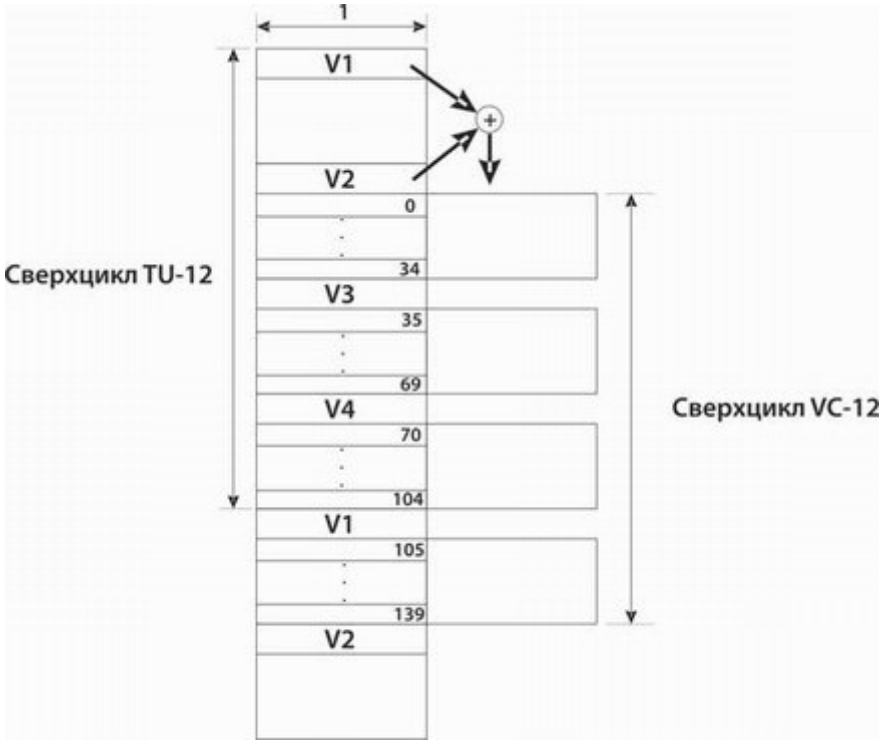
Байты H3 являются резервными байтами для передачи информации в момент отрицательного выравнивания.

Указатели TU-3 PTR используются при варианте размещения трех контейнеров VC-3 в одном контейнере VC-4. В этом случае из виртуального контейнера VC-3 образуются

группа трибутарного блока TUG-3 путем добавления 3-х байтного указателя (TU-3 PTR) и 6 фиксированных байтов выравнивания.



На рисунке представлена схема адресации с помощью указателей TU-3 PTR. В контейнере VC-4, вслед за байтами маршрутного заголовка POH и фиксированными байтами выравнивания, следуют по-байтно мультиплексированные три группы TUG-3. Диапазон адресов начала контейнера VC-3 внутри группы TUG-3 простирается от 0 до 764. В примере на этом рисунке первый контейнер VC-3 начинается с адреса 0, второй контейнер - с адреса 85, а третий - с адреса 594. Структура байтов H1, H2 и H3 указателя TU-3 PTR полностью совпадает со структурой AU-4 PTR и используется аналогичный механизм выравнивания фаз и скоростей сигналов.



Как ранее указывалось, виртуальные контейнеры VC-12 свехцикла образуют сверхцикл TU-12 при добавлении указателя TU-12 PTR. Роль этого указателя аналогична указателям AU-4 PTR и TU-3 PTR, а именно зафиксировать начало виртуального контейнера. В данном случае - начало сверхцикла виртуальных контейнеров VC-12. На рисунке изображено размещение сверхцикла VC-12 в свехцикле TU-12. Назначение и структура байтов V1, V2 и V3 такое же как байтов H1, H2 и H3. Отличие заключается в только в битах SS. Для рассматриваемого класса указателей значения этих битов несут смысловую нагрузку и определяют идентифицируют конкретный тип указателя. Для TU-11 PTR значение должно равняться “11”, для TU-12 PTR - “10” и для TU-2 PTR - “00”. Десятиразрядное поле значения указателя TU-12 PTR может содержать значение от 0 до 139. Из этого следует, что сверхцикл VC-12 может быть передан с помощью 4-х или 5-ти циклов STM-1. В примере на рисунке значение указателя равно 0, т.е. сверхцикл VC-12 начинается сразу за байтом V2 указателя и для его передачи потребуется только 4 цикла STM-1. Байт V3 являются резервным и служит для передачи информации в момент отрицательного выравнивания. Механизм выравнивания аналогичен рассмотренным выше. При передаче виртуальных контейнеров VC-12 в цикле STM-1 используется еще один специальный указатель. Это так называемый NPI указатель, появляющийся на месте указателя TU-3 PTR при объединении контейнеров VC-12 в группу TUG-3. В NPI указателе поле флага новых данных содержит активный статус (“1001”), а десятиразрядное поле значения указателя имеет постоянное, ничего незначащее значение - “1111100000”. Байт H3 естественно не используется в этом случае, так как все процедуры выравнивания осуществляются на уровне указателей TU-12 PTR.

Заголовки контейнеров и сигналов (overhead)

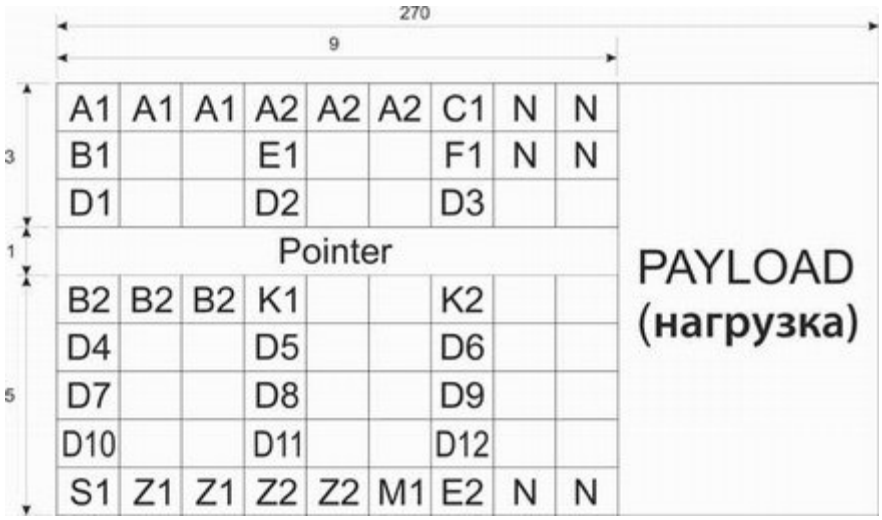
Заголовки играют важную роль в процессе передачи полезной информации с помощью циклов SDH. Заголовок всегда отделен от передаваемой нагрузки. Благодаря этому байты заголовка могут быть считаны, изменены или дополнены без затрагивания самой информации.

Известно, что заголовок цикла STM-1 состоит из трех частей:

- PTR - указатель административного блока (AU), определяющий положение отдельных уплотненных сигналов (контейнеров VC-4 и VC-3) в цикле STM-1.
- RSOH - заголовок регенерационной секции, содержащий сигналы управления, контроля и цикловой синхронизации для обеспечения работоспособности участков регенерации.
- MSOH - заголовок мультиплексорной секции, обеспечивают взаимодействие между мультиплексорами. Через регенераторы проходят без изменений.

Совместно RSOH и MSOH составляют секционный заголовок (SOH -Section Overhead). За счет этого заголовка в сигнале STM образуются сети управления и синхронизации, которые обеспечивают передачу сигналов синхронизации, сетевого управления, мониторинга и технического обслуживания, поддерживают служебные каналы связи.

На рисунке представлена карта распределения байтов заголовков RSOH и MSOH.



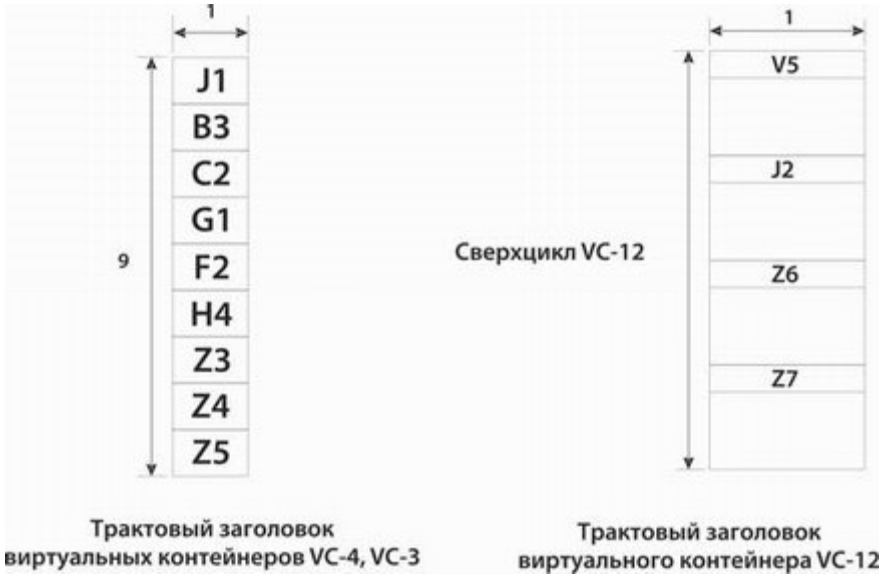
Рассмотрим назначения этих байтов:

- A1, A2 - сигналы выравнивания, цикловая синхронизация. Байт A1 содержит значение “11110110”, A2 - “00101000”.
- B1 - контроль ошибок регенерационной секции. Этот байт (контроль четности) создается на базе всех бит предыдущего цикла после скремблирования и записывается в текущем цикле до скремблирования.

- B2 - контроль ошибок мультиплексорной секции. Данные байты формируются на базе всего нескремблированного цикла за исключением байтов, входящих в заголовок RSOH. Результат записывается в соответствующие позиции перед скремблированием.
- C1 - идентификатор цикла STM-1. Присваивается каждому STM-1 перед уплотнением в STM-N.
- D1 - D3 - образуют канал передачи данных со скоростью 192 кбит/с в регенерационных секциях (DCC-R). Используются только в первом STM-1 цикла STM-N. Канал DCC-R служит для передачи управляющих команд и сигналов контроля между регенераторами и центром управления сетью.
- D4 - D12 - образуют канал передачи данных со скоростью 576 кбит/с в мультиплексорных секциях (DCC-M). Используются только в первом STM-1 цикла STM-N. Канал DCC-M создает линию связи между мультиплексорами и центром управления согласно рекомендации ITU-T G.784.
- E1 - образует локальный служебный канал, который используется для речевой связи между регенераторами.
- E2 - аналогично E1, только между мультиплексорами.
- F1 - канал оператора сети SDH. Предусматривается для собственных нужд, возможна передача данных или речи. Используются только в первом STM-1 цикла STM-N.
- K1, K2 - байты сигнализации в системе автоматического переключения на резерв (APS). Используются только в первом STM-1 цикла STM-N. Кроме функции обеспечения автоматического переключения в байте K2 биты 6, 7 и 8 устанавливаются в “1” при передачи сигнала аварии AIS (Alarm Indication Signal). Поясним назначение сигнала AIS, он формируется если обнаружена ошибка, например потеря цикловой синхронизации STM-1 - секционный AIS или ошибка в виртуальном контейнере - трактовый AIS. Сформированный AIS посылается в том же направлении передачи как и неискаженные сигналы. Его цель - предотвратить генерацию сигналов аварии в последующем оборудовании. Если приемник мультиплексора не принимает сигнал или был принят сигнал AIS, то через биты 6, 7, 8 байта K2 передается комбинация “110”. Таким образом удаленной стороне сообщается об ошибках приема.
- S1 - служит для индикации наличия синхросигнала (например, от мастер-генератора) во входящем потоке STM-N. Используются только в первом STM-1 цикла STM-N.
- M1 - называется FEBE (Far End Block Error) и содержит число блоков с ошибками, обнаруженными с помощью байтов B2. Для STM-1 имеют смысл значения от 0 до 24, а для STM-4 - от 0 до 96. Остальные значения не должны формироваться.

- Z1, Z2 - зарезервированы для еще неопределенных функций.
- N - зарезервированы для национального применения.
- Остальные байты зарезервированы для будущего использования.

Кроме секционного заголовка SOH рекомендации ETSI определяют три вида трактовых заголовков (POH -Path Overhead), это VC-4 POH, VC-3 POH и VC-12 POH. Заголовок POH добавляется к соответствующим контейнерам C, образуя виртуальные контейнеры. На рисунке ниже приведены байты данных заголовков.



Рассмотрим назначение указанных байтов для VC-4 POH и VC-3 POH:

- J1 - этот байт является первым байтом виртуального контейнера и служит для передачи 64-байтной информации о трассе прохождения такого контейнера. Передача этой информации осуществляется циклически по одному байту в течении каждых 64 циклов.
- B3 - контрольный байт для обнаружения ошибок в виртуальном контейнере. Перед процедурой скремблирования виртуального контейнера по всем его байтам вычисляется данный контрольный байт, используется метод контроля четности. Сформированный байт записывается в поле B-3 последующего контейнера опять же перед процедурой вычисления контрольного байта и скремблированием.
- C2 - сигнальная метка. Служит для индикации содержимого виртуального контейнера. Определены следующие значения этой метки:

- C2 = 00h - тракты контейнеров VC-3 и VC-4 не сформированы.
- C2 = 01h - тракты контейнеров VC-3 и VC-4 сформированы, но отсутствует полезная информация.
- C2 = 02h - тракт VC-4 сформирован для передачи 3-х групп TUG-3.
- C2 = 12h - тракт VC-4 сформирован для передачи сигнала 140 Мбит/с.

- C2 = 13h -тракт VC-4 сформирован и служит для передачи ячеек ATM.
- Все остальные значения зарезервированы для будущих применений.

- G1 - данный байт используется для сигнализации ошибок в обратном направлении. С помощью этого байта в сторону начала тракта передается сообщение о его состоянии и качественных показателей. Первые четыре бита называются FEBE (Far End Block Error) и передают число дефектных блоков, определенных с помощью контрольного байта B3. Имеют смысл значения от 0 до 8, все остальные интерпретиру.тся как 0, т.е. как отсутсвие ошибок. Пятый бит является индикатором аварии и называется FERF (Far End Receive Failure) и устанавливается в “1” при приеме AIS, пропадании или ошибки в сигнале, при неправильно сформированных сквозных трактах. Остальные биты байта G1 неиспользуются.
- F2, Z3 - зарезервированы для целей организации служебных линий связи оператора сети. В настоящее время еще нет точной спецификации этой возможности.
- H4 - индикатор (счетчик) положения полезной информации, распределенной по нескольким циклам (сверхцикл при передачи виртуального контейнера VC-12). С помощью этого индикатора можно определить наличие сверхцикла и идентифицировать отдельные циклы сверхцикла.
- Z4 - не используется, зарезервирован.
- Z5 - зарезервирован для эксплуатационных целей. Используется оператором сети как для подсчета входящих ошибок, так и для организации канала связи.

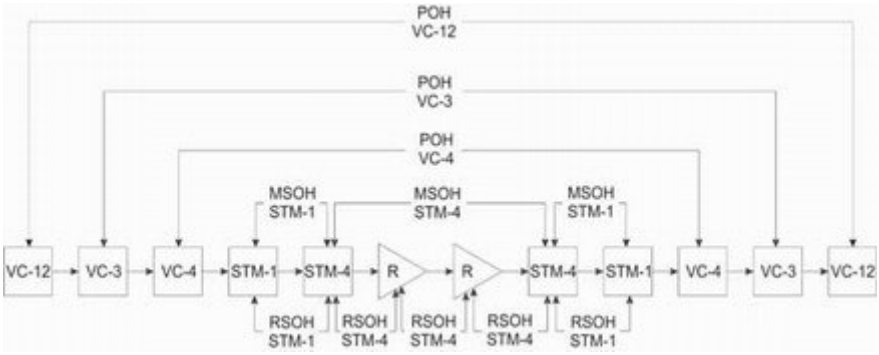
Трактовый заголовок виртуального контейнера VC-12 формируется в процессе передачи сверхцикла и состоит из четырех байтов. Ранее на рисунке приводится распределение этих байтов в составе сверхцикла.
V5 - данный байт заголовка служит для обнаружения ошибок, передает сигнальную метку и показывает состояние тракта. Для каждой задачи предопределены соответствующие биты этого байта. Биты 1 и 2 используются для обнаружения ошибок методом контроля четности. Бит 1 обеспечивает контроль четности нечетных (по счету в байте - 1, 3, 5 и 7) битов всех байтов предыдущего виртуального контейнера VC-12. Соответственно, бит 2 используется для контроля четности четных (по счету в байте - 2, 4, 6 и 8) битов. Контроль четности не производится по байтам V1, V2, V3 и V4, образующих указатель TU-12. Исключением является байт V3 в случае наличия отрицательного выравнивания. Бит 3 является индикатором FEBE, устанавливается приемной стороной и оценивается передающей. Является своего рода обратной связью. При обнаружении хотя бы одной ошибки с помощью 1 и 2 бита он устанавливается в значение “1” и этим сообщаеттся источнику тракта о наличии ошибок. Если ошибки не были обнаружены, то его состояние -”0”. Бит 4 не используется. Биты 5, 6 и 7 передают сигнальную метку. Значение “000” сообщает, что тракт контейнера

VC-12 не сформирован. Значение “001” - тракт сформирован, но не определен (передается не стандартный сигнал). Значение “010” - передается асинхронный сигнал. Значение “100” - передается синхронный сигнал. Остальные комбинации значений (“101”, “110”, “111”) сообщают, что тракт сформирован и зарезервирован для использования в будущем. Бит 8 является индикатором аварии, сигнал FERF. Устанавливается в “1” и сообщает передающей стороне о пропадании сигнала или о приеме AIS.

J2 - используется для передачи трактовой метки, позволяющей отслеживать непрерывность соединения по тракту.

Z6, Z7 - зарезервированы для будущего использования.

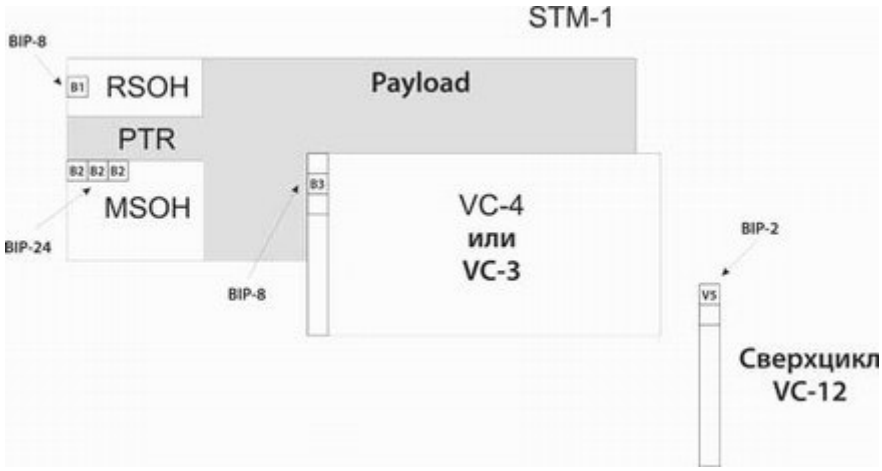
На рисунке представлены участки “ответственности” каждого типа заголовка.



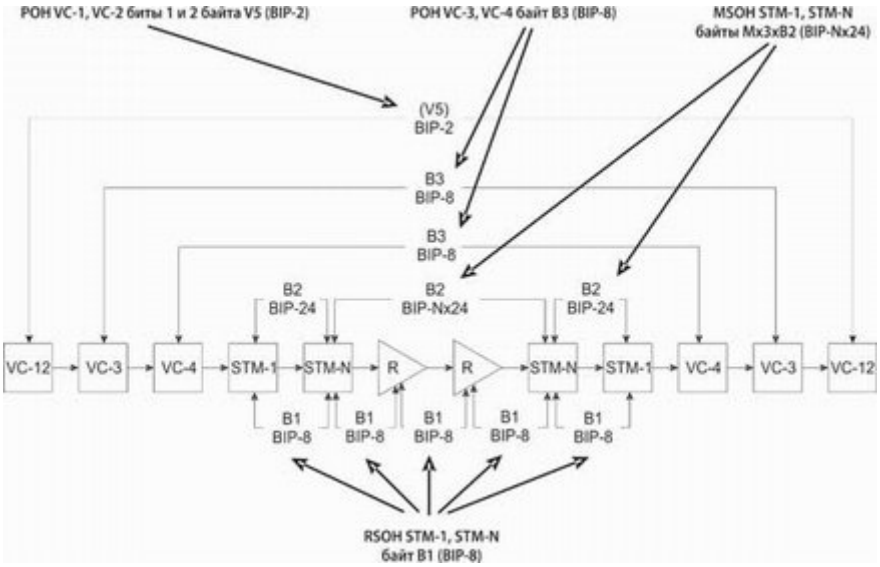
Контроль ошибок и управление в сетях SDH

С помощью соответствующих байтов и битов заголовков циклов STM и виртуальных контейнеров осуществляются процедуры контроля и управления на сети SDH.

Для обнаружения битовых ошибок используется процедура контроля четности или BIP (Bit Interleaved Parity). Эта процедура основывается на методе добавления “1” до четного числа. Если в некой битовой последовательности присутствует нечетное число “1”, то в контрольном разряде устанавливается дополнительная “1”. И наоборот, если число “1” - четное, то в контрольном разряде устанавливается “0”. В SDH для обеспечения контроля по четности используются кодовые слова различной длины. Принцип формирования этих слов одинаков. Вся контролируемая битовая последовательность условно разбивается на блоки, равные длине конкретного кодового слова. Затем полученные блоки складываются побитно в соответствии с правилом “исключающего ИЛИ”. Полученный результат представляет собой искомое контрольное кодовое слово. Другими словами, происходит подсчет числа “1”, стоящих на соответствующих битовых позициях. Полученное кодовое слово передается в соответствующем заголовке следующего цикла STM или виртуального контейнера. На приемной стороне вновь вычисляется кодовое слово и сравнивается с принятым словом из последующего информационного блока. Если эти слова совпали, то делается вывод о приеме без искажений. Используемые в SDH кодовые слова приведены на рисунке:



На участке регенерационной секции используется слово BIP-8, располагающееся в байте B1 заголовка RSOH. Это слово формируется из всех битов цикла после операции скремблирования и помещается в байт B1 следующего цикла перед скремблированием. Напомним, что операции скремблирования подвергается весь кадр за исключением первых 9 байт заголовка RSOH. Слово BIP-8 проверяется в каждом мультиплексоре и регенераторе. На участке мультиплексорной секции используется кодовое слово BIP-24, которое располагается в байтах B2 заголовка MSOH. Это справедливо для цикла STM-1. При использовании STM-N кодовое слово будет равно BIP-Nx24. Кодовое слово BIP-24 формируется перед операцией скремблирования из всего цикла STM-1 за исключением первых 3-х рядов SOH (это RSOH). Полученное значение помещается в байты B2 следующего цикла перед его скремблированием. Таким образом, значение BIP-24 не изменяется в регенераторах. Для виртуальных контейнеров VC-3 и VC-4 используется кодовое слово BIP-8, располагающееся в байте B3 трактового заголовка POH. Это слово формурется из всех битов виртуального контейнера и помещается в POH следующего контейнера. При формировании BIP-8 не учитываются биты указателя. Для виртуального контейнера VC-12 используется кодовое слово BIP-2, которое размещается в битах 1 и 2 байта V5 трактового указателя POH. Слово BIP-2 формируется из всего сверхцикла VC-12 и размещается в последующем сверхцикле. На рисунке показаны действия каждого типа BIP.



Принимаемая сторона формирует несколько типов сигналов, несущих аварийную информацию. Имеются два вида сигналов - индикаторов ошибок. Это FEBE (Far End Block Error) - ошибка блока на дальнем конце и FERF (Far End Receive Failure) - отказ при приеме на дальнем конце. Различают путевые и секционные сигналы.
Для начала рассмотрим условия формирования сигнала FEBE. Этот сигнал посылается передающей стороне для уведомления об обнаруженных ошибках с помощью кодовых слов BIP.

Для передачи трактового FEBE виртуальных контейнеров VC-3 и VC-4 используются биты 1 - 4 байта G1 заголовка POH. Для BIP-8 максимально может быть обнаружено 8 нарушений четности. Код FEBE содержит число таких нарушений и может принимать значение от 0 до 8. Все другие значения интерпретируются как 0.
Бит 3 байта V5 трактового заголовка POH используется для передачи FEBE виртуального контейнера VC-12. Если этот бит равен “0”, то нарушений четности в кодовом слове BIP-2 не было обнаружено. Для передачи секционного FEBE цикла STM-1 используется байт M1 заголовка MSOH. Для STM-1 значение FEBE может быть от 0 до 24, а для STM-N - от 0 до Nx24.

Сигнал FERF посылает уведомление передающей стороне об обнаружении на приемной стороне сигнала AIS или о невозможности осуществлять прием. Здесь речь идет о приеме сигналов от миультиплексоров SDH, расположенных далее по цепочке. Т.е. сигнал аварии FERF двигается сонаправлено передаваемому сигналу.

Для виртуальных контейнеров VC-3 и VC-4 путевой сигнал FERF передается в бите 5 байта G1. Для этого он устанавливается в “1”. Для виртуального контейнера VC-12 сигнал FERF передается битом 8 байта V5. Трактовый сигнал FERF устанавливается, если:

- для BIP-8 норма битовых ошибок (Bit Error Rate) BER больше или равен 10^{-4};

- имеется ошибка в байте J1, искажение информации о трассе прохождения виртуального контейнера;
- отсутствует сигнал виртуального контейнера.

Сигнал FERF для STM-1 передается в битах 6 - 8 байта К2, значение равно 110. Секционный FERF устанавливается, если:

- для BIP-24 значение BER больше или равен 10^{-3};
- обнаружен сигнал AIS в секционном заголовке;
- потеря сигнала цикловой синхронизации FAS;
- потеря сигнала STM-1.

Сигнал AIS (Alarm Indication Signal) - сигнал индикации аварийного состояния формируется при обнаружении целого ряда ошибок в принимаемом сигнале. Цель сигнала AIS -предотвратить генерацию сообщений об ошибках в последующих по цепочке мультиплексорах или регенераторах. Прием сигнала AIS вызывает ответные действия (такие как блокировка канала) только в определенном терминальном оборудовании. Сигнал AIS используется в PDH и SDH. В SDH при обнаружении сигнала AIS цикл STM-1 или STM-N полностью сохраняется и передается далее. В PDH этот сигнал показывает невозможность цикловой синхронизации FAS на дальнейших участках. Это происходит потому, что байты цикловой синхронизации и сложебное слово PDH заполняются лог. “1” для предачи сигнала AIS. В SDH различают трактовый AIS и секционный AIS. Трактовый AIS соответствует виртуальным контейнерам иерархии SDH. Для трибутарных блоков TU - 1, 2, 3 указатель устанавливается в “1” в случае AIS TU. Для административных блоков AU - 3, 4 указатель устанавливается в “1” при AIS AU. Эти постоянные сигналы передаются в цикле STM-1 как искаженные трибутарные блоки. Трактовый AIS устанавливается, если:

- для BIP-8 значение BER больше или равен 10^{-4};
- имеется ошибка в байте J1;
- отсутствует сигнал виртуального контейнера;
- был принят AIS от предыдущего оборудования.

Секционный AIS передается путем установки бит 6 -8 байта К2 в “1”. Устанавливается , если искажены циклы STM-1 или STM-N. Условия:

- был принят секционный AIS от предыдущего оборудования;
- повреждение в мультиплексоре или регенераторе;
- потеря сигнала цикловой синхронизации FAS;
- потеря сигнала STM-1.

Оборудование SDH допускает как централизованное управление с помощью единого сетевого центра управления, так и автономное с помощью локального управляющего терминала.

Сигналы управления и контроля на сетях SDH передаются в заголовках RSOH и MSOH с помощью D байтов. В цикле STM-N для передачи этих сигналов используются D байты только первого STM-1. Для организации технологической связи между составными частями территориально распределенной сети SDH используются каналы речевой связи. Эти каналы образуются за счет E байтов заголовков RSOH и MSOH.