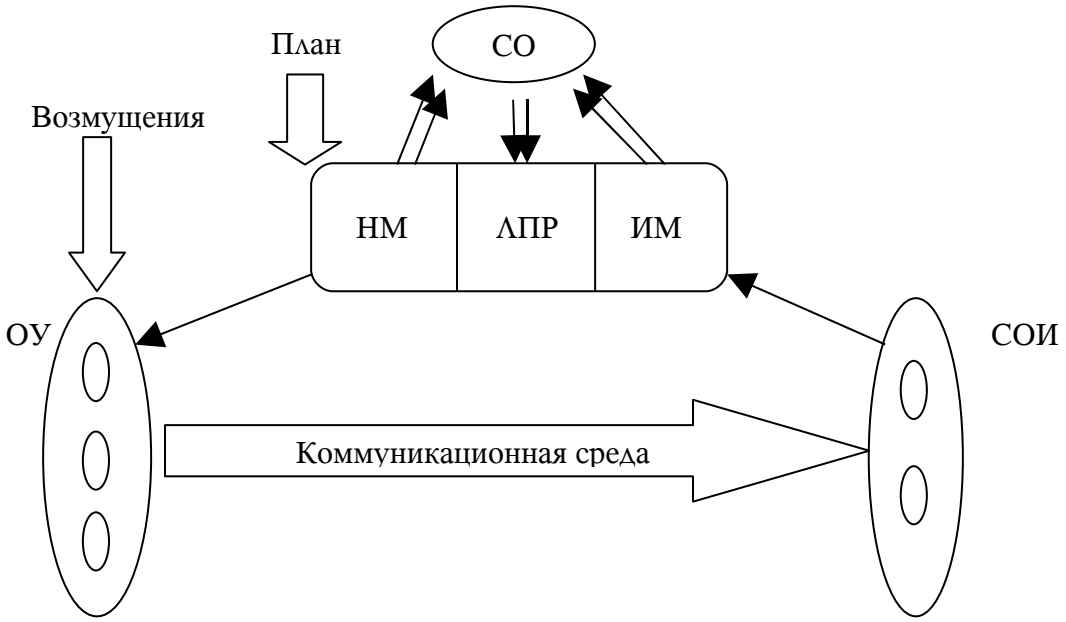
1. Структурная схема распределенной системы управления



СО – сигнал ошибки (рассогласования);

НМ – нормативная модель (план);

ЛПР – лицо принимающее решения;

ИМ – информационная модель;

ОУ – объект управления;

СОИ – система обработки информации.

2. Сети ЭВМ – частный случай распределенных систем

Информационная система – человеко-машинная система для производства *информационных продуктов*, использующая компьютерную информационную технологию.

Информационная технология – совокупность чётко определенных целенаправленных действий персонала по переработке информации на компьютере (компьютерах).

В информационных системах различают сильные и слабые связи между элементами:

- **Сильные аппаратные связи** – все процессоры разделяют общую оперативную (ОП) память;
- **Слабые аппаратные связи** – каждый процессор имеет отдельную ОП;
- **Сильные программные связи –** единая операционная система (ОС), под ее управлением любой процесс может выполняться на любом процессоре;
- **Слабые программные связи –** каждый компьютер имеет свою ОС.

Сильные связи характерны для ***мультипроцессорных систем***.

Процессоры расположены в едином конструктиве (корпусе). *Пример:* кластеры - однородная вычислительная система, выполненная на процессорных неразрезных матрицах (СБИС). Производительность –E13 –E14 флопов/с (специальных элементарных команд). Распределенная обработка в смысле распараллеленная, но пространственно как бы сосредоточенная.

Слабые связи - *вычислительных сетей (сети ЭВМ).*

- Основные элементы – стандартные компьютеры, *не имеющие общей ОП*; каждый компьютер имеет *свою собственную ОС*.
- Системная (сетевая) часть – оболочка или встроенная ОС.
- Взаимодействие между компьютерами – механизм обмена сообщениями через каналы связи (КС).

Разделение локальных ресурсов каждого компьютера между всеми пользователями сети является *целью создания сети* (ресурсы – диски, файлы, принтеры, модемы, факс – аппараты).

Программными серверами (serve – обслуживать) называют специальные программные модули в режиме ожидания запросов.

Программными клиентами (client) называют специальные программные модули, вырабатывающие запросы.

Это части операционных систем.

Пара клиент-сервер, обеспечивая доступ к определенному ресурсу, «образует» определенную службу:

- файловая служба;
- служба печати;
- служба электронной почты;
- служба удаленного доступа, и др. (прикладной уровень ЭМ ВОС).

Термины «клиент», «сервер» используются и для обозначения компьютеров.

Многомашинные системы – это вычислительный комплекс, включающий в себя несколько компьютеров, аппаратные и программные средства связи, обеспечивающие работу комплекса как единого целого.

У каждого компьютера:

- *собственные ОП и ОС;*
- *системное ПО* предоставляет пользователям *прозрачный доступ* к ресурсам всех компьютеров, входящих комплекс;
- в состав средств связи входят *программные модули*, которые занимаются *распределением вычислительной нагрузки, синхронизацией вычислений, реконфигурацией системы*

Связь между компонентами менее тесная, чем у мультипроцессорной системы, т.к. *обмен сообщениями осуществляется* не через общее поле памяти (ОПП), а через *периферийные многовходовые устройства*.

В отличие от сетей территориальная распределённость не обеспечивается, поскольку расстояния между компьютерами определяются длиной связи между процессорным блоком и дисковой подсистемой.

Особенности информационных сетей как распределенных систем

Сеть ЭВМ – набор аппаратных и программных средств, обеспечивающих соединение компьютеров и позволяющих им использовать общие ресурсы и обмениваться данными.

В технологии «клиент – сервер» клиентская программа ***РЕДИРЕКТОР*** способна отличить запрос к удаленному файлу от запроса к локальному.

АДРЕСАЦИЯ КОМПЬЮТЕРОВ *в сети.*

Адрес - уникальный идентификатор компьютера в сети.

Три схемы адресации:

- ***Аппаратные адреса*** (hardware) (физический адрес). Для сети небольшого размера. Без иерархии. Малого размера. Встраивается в аппаратуру изготовителем (заводской номер изделия). Не удобен, при замене компьютеров.
- ***Символьные адреса*** (имена). Запоминать легче. В больших сетях могут быть иерархическими. Передача по сети не очень удобна (разная длина, может быть большой).
- ***Числовые составные адреса***. В больших сетях. Адреса фиксированного и компактного форматов. Двух и трех уровневые иерархии: № сети, № узла, (№ процесса).

В современных сетях используются одновременно все три схемы: пользователи адресуют компьютеры ***символьным****и* именами (адресами), которые автоматически заменяются на ***числовы****е* при передаче по составной сети. При входе в локальную сеть численный адрес преобразуется в ***аппаратный***. Специальная служба - ***служба разрешения имен*** – содержит соответствия (таблицы) между различными схемами адресации (таблицы хранятся на сервере имен).

СТРУКТУРИЗАЦИЯ СЕТЕЙ.

Типовые топологии сетей: шина, кольцо, звезда, ячеистая, сотовая.

СТРУКТУРИЗАЦИЯ сетей включает ограничения при построении больших сетей:

- на длину связи между узлами;
- на количество узлов в сети;
- на интенсивность трафика, порождаемого узлами.

ФИЗИЧЕСКАЯ СТРУКТУРИЗАЦИЯ предполагает *конфигурацию связей*, образованных отдельными частями кабеля. Реализуется с помощью коммуникационных устройств:

- повторитель (repeator),
- концентратор (concentrator)
- хаб (hub).

ЛОГИЧЕСКАЯ СТРУКТУРИЗАЦИЯ предполагает конфигурацию информационных потоков между компьютерами сети (термин – логическая сегментация). Реализуется устройствами:

- мостами,
- коммутаторами,
- маршрутизаторами,
- шлюзами.

СЕТЕВЫЕ СЛУЖБЫ.

Для пользователя сеть – это набор сетевых служб.

Сеть, кроме обмена данными, решает и другие задачи:

- ***служба репликации*** – обеспечивает непротиворечивость копий на разных компьютерах;
- ***служба администрирования учетных записей о пользователях*** – ведет общую базу данных;
- ***служба мониторинга сети*** – захват и анализ трафика, и др.

Реализуются программами. Решаемые проблемы:

- определение протокола взаимодействия между клиентской и серверными частями;
- распределение функций между ними;
- выбор схемы адресации приложений, и др.

Для пользователей обеспечивается ***прозрачный доступ***.

3. Классификация сетей

Признаки классификации:

- Территориальная распространенность («охватываемость»);
- Ведомственная принадлежность;
- Скорость передачи информации;
- Тип среды передачи.

По территориальному признаку различают:

- LAN (Local Area Network) – локальная сеть;
- MAN (Metropolitan Area Network) – региональная (городская) сеть;
- WAN (Wide Area Network) – глобальная сеть.

LAN – охватывает площадь, не превышающую 10 км^2.

- Компьютер, подключенный к сети, называется ***рабочей станцией*** (Workstation).
- Общие ресурсы в качестве услуг предоставляются ***серверами***.
- Рабочие станции (PC), обращающиеся за услугами к серверам, называются ***клиентами***.
- Реализацию обращений за ресурсами и их предоставление (доставку) обеспечивает ***коммуникационная система*** (КС).

Технология «клиент – сервер» доминирует в ЛС. Потребитель ресурса – *клиент*. Поставщик ресурса – *сервер*.

Ресурс: аппаратный элемент, программы (приложения), файлы, сообщения, ЭВМ в целом.

Базовые технологии ЛС – Ethernet, Tokin Ring (широкого развития не получила).

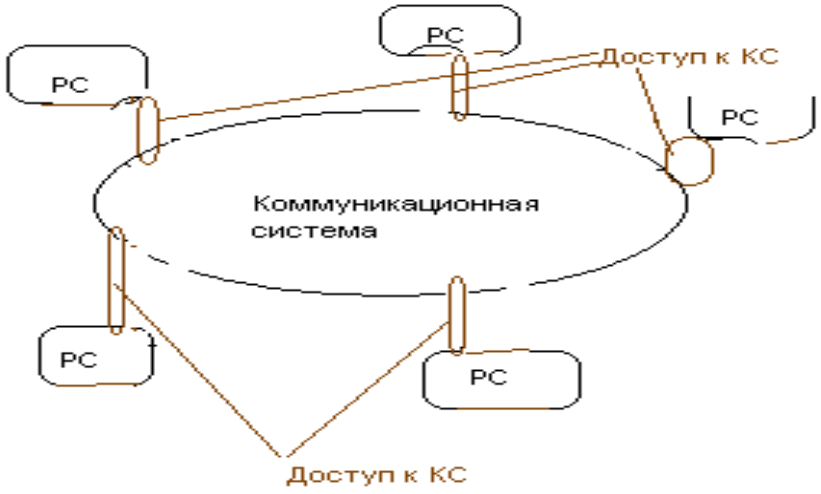


Рис. 1.1. Структура локальной сети

WAN (Глобальная сеть) – обеспечивает предоставление информационных услуг многочисленным территориально распределенным пользователям. Распределение пользователей может быть в пределах мегаполиса, региона, государства, континента, земного шара в целом.

Глобальная сеть обеспечивает более широкий спектр пользователей. Их взаимодействие – через коммуникационную систему, которая представляет собой телекоммуникационную сеть (общественную, ведомственную, частную).

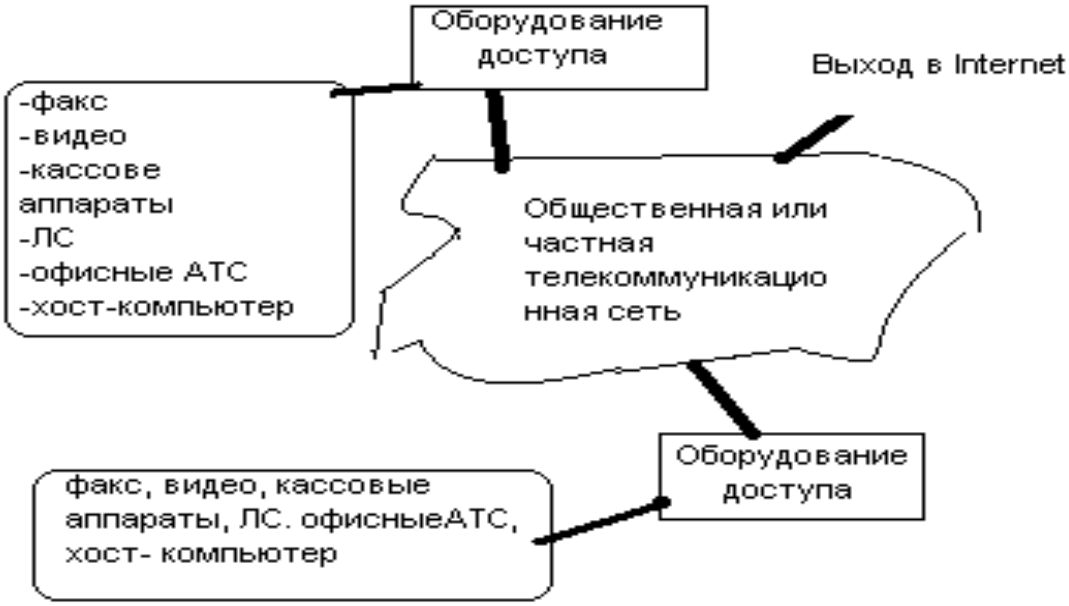


Рис. 1.2. Глобальная сеть как транспортное средство

Глобальная сеть – это транспортное средство, предлагающее услуги по обмену информацией, включает все 7-м уровней ЭМ ВОС.

Структура глобальной сети – это множество узлов коммутации, соединенных магистральными каналами связи.

Примеры сетей:

- Общедоступные сети передачи данных - ПД (PDN) типа X.25 (TELNET, TYMNET, РОСПАК – федеральная государственная сеть общего пользования, INFOTEL, POCHET);
- «Спринт – сеть».

Эти сети решали задачу доступа удаленных ЭВМ и терминалов к мощным ЭВМ (HOST-ам). У таких сетей были низкие скорости.

Устойчивая тенденция глобальной сети – ***интегральное обслуживание***.

Результат оцифрования телефонной сети – сеть ISDN (Integrated Services Digital Network) (70-е годы XX века) и, позднее, BISDN (Broadband ISDN) – широкополосная (высокоскоростная) сеть с дополнительными информационными услугами: гипертексты, звукозаписи, видео и телепрограммы, интербеседы.

Другие сети с повышенной скоростью:

- DECnet (фирмы DEC), 5- (Phase V) – ISDN/OSI //OSI – Open Systems Interconnection
- Frame Relay («реле блока данных»). Замышлялась как протокол для использования в интерфейсе ISDN (быстрая коммутация пакетов);
- Apple Talk (Phase II) – патентованная сеть;
- ATM –Asynchronous Transfer Mode (Асинхронный метод доставки).

MAN занимают промежуточное положение между **LAN** и **WAN.**

4. Эталонная модель взаимодействия открытых систем (ЭМВОС) – OSI (Open System Interconnection)

1980 г. - Международная Организация по Стандартизации (International Standards Organization, ISO) признала необходимость в создания модели сети, которая могла бы помочь поставщикам создавать реализации взаимодействующих сетей.

1984 г. – выпущена эталонная модель "Взаимодействие Открытых Систем" (Open System Interconnection, OSI).

Суть сети – совместимость возможна на основе принятия всеми производителями общепринятых правил построения сетевого оборудования, закрепление «нового» в соответствующем **стандарте.**

Идеологическая основа стандартизации – *многоуровневой подход к разработке средств сетевого взаимодействия:* разработана стандартная *семиуровневая модель* – универсальный язык сетевых специалистов.

При передаче сообщений оба участника сетевого обмена должны принять множество соглашений:

- согласовать уровни и форму электрических сигналов,
- способ определения длины сообщений,
- договориться о методах контроля достоверности и т.п.

Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого уровня передачи битов, до самого высокого уровня, детализирующего, как информация должна быть интерпретирована.

Протоколами называют такие формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах.

Стеком коммуникационных протоколов называют иерархически организованную совокупность протоколов, решающих задачу взаимодействия узлов сети.

Протоколы соседних уровней, находящихся в одном узле, взаимодействуют друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть *интерфейсом.* Интерфейс определяет набор услуг, которые нижележащий уровень предоставляет вышележащему.

ISO/OSI - четко определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень.

Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Следует иметь ввиду что приложение может взять на себя функции некоторых верхних уровней модели OSI, в таком случае при необходимости обмена данными оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

Приложение конечного пользователя может использовать системные средства взаимодействия не только для организации диалога с другим приложением, выполняющимся на другой машине, но и просто для получения услуг того или иного сетевого сервиса, например, доступа к удаленным файлам, получение почты или печати на разделяемом принтере.

Рис. 1.3. Модель взаимодействия открытых систем ISO/OSI

Пусть приложение обращается с запросом к прикладному уровню, например к файловому сервису. На основании этого запроса программное обеспечение прикладного уровня формирует сообщение стандартного формата, в которое помещает служебную информацию (заголовок) и, возможно, передаваемые данные и так далее по нисходящей. Наконец, сообщение достигает самого низкого, физического уровня, который действительно передает его по линиям связи.

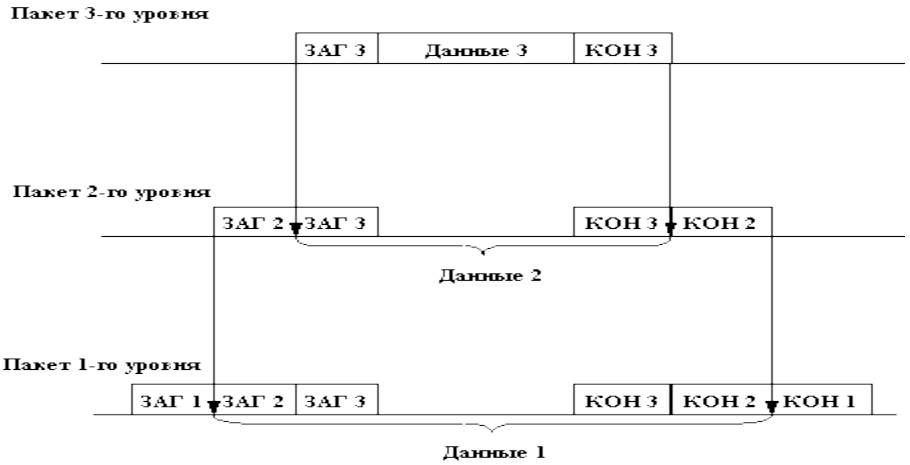


Рис. 1.4. Вложенность пакетов различных уровней

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.

В модели OSI различается два основных типа протоколов:

- *С установлением соединения* (connection-oriented network service, CONS) – перед обменом данными отправитель и получатель должны сначала установить соединение и, возможно, выбрать протокол, который они будут использовать. После завершения диалога они должны разорвать это соединение.

- *Без предварительного установления соединения* (connectionless network service, CLNS) (*дейтаграммными* протоколами) – отправитель просто передает сообщение, когда оно готово; при взаимодействии компьютеров используются как те, так и другие протоколы.

Эталонная модель OSI была разработана прежде, чем были изобретены протоколы для нее, поэтому и не была настроена на какой – то конкретный набор протоколов, что сделало ее ***универсальной***.

Обратная сторона – у разработчиков не было четкого представления, какие функции должен выполнять каждый уровень.

Еще до появления модели OSI внедрена в практику Internet модель TCP/IP. С этой моделью было все наоборот: сначала протоколы, потом модель, описывающая существующие протоколы. Поэтому не было проблемы с соответствием протоколов модели. Проблем оказалась в другом – модель не соответствовала никаким другим стекам протоколов. Поэтому не используется для описания каких либо других сетей, кроме TCP/IP.

Различия моделей OSI и TCP/IP:

1. Количество уровней

OSI	**TCP/IP**
Прикладной	Прикладной
Представительный	Не присутствует
Сеансовый	Не присутствует
Транспортный	Транспортный
Сетевой	Межсетевой
Канальный,	От хоста к сети
Физический	От хоста к сети

2. OSI на сетевом уровне поддерживает возможности использования связи с *установлением соединения* и *без установления соединения*, на транспортном уровне – только на основе *установления соединения.*
3. TCP/IP – на сетевом уровне только без *установления соединения, на транспортном уровне* – оба режима, предоставляя пользователю выбор.

В заголовке содержится информация о том, как обрабатывать данный информационный блок.

Концепция заголовка и собственно данных относительна и зависит от перспективы того уровня, который в данный момент анализирует информационный блок. Например, в *Уровне 3* информационный блок состоит из заголовка *Уровня 3* и следующими за ним данными. Однако данные *Уровня 3* могут содержать заголовки *Уровней 4, 5, 6 и 7*. Кроме того, заголовок *Уровня 3* является просто данными для *Уровня 2*. И наконец, не все уровни нуждаются в присоединении заголовков. Некоторые уровни просто выполняют трансформацию фактических данных, которые они получают, чтобы сделать их более или менее читаемыми для смежных с ними уровней.

Модель ISO/OSI определяет функции уровней следующим образом:

Физический уровень.

Этот уровень имеет дело с передачей битов по физическим каналам:

- Коаксиальный кабель;
- Витая пара;
- Оптоволоконный кабель.

К этому уровню имеют отношение характеристики физических сред передачи данных:

- 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. Повторители являются единственным типом оборудования, которое работает только на физическом уровне.

Примером протокола физического уровня может служить спецификация 10Base-T технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную витую пару категории 3 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100

метров, манчестерский код для представления данных на кабеле, и другие характеристики среды и электрических сигналов.

Канальный уровень.

Задачи:

- ***Проверка доступности среды передачи.***

  На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются попеременно (разделяются) несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята.

- ***Реализация механизмов обнаружения и коррекции ошибок.***

  Для этого на канальном уровне биты группируются в наборы, называемые *кадрами (frame)*. 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.

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*.

Сетевой уровень.

Протокол канального уровня обеспечивает доставку данных между любыми узлами только в сети с соответствующей *типовой топологией*. Это очень 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. Для того, чтобы, с одной стороны сохранить простоту процедур передачи данных для типовых топологий, а с другой – стороны допустить использование произвольных топологий, вводится дополнительный сетевой уровень. На этом уровне вводится более узкое понятие "*сеть*". 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 регулируется *канальным уровнем*, а доставкой данных между сетями занимается *сетевой уровень*.

Сообщения сетевого уровня принято называть "пакетами" (packet).

При организации доставки пакетов на сетевом уровне используется понятие "*номер сети"*.

Адрес получателя: № сети + № компьютера в этой сети.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.

Маршрутизатор - это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения.

Для того, чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Главная задача сетевого уровня: выбора наилучшего пути пакета (*маршрутизация*).

«Самый короткий путь не всегда самый лучший».

Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от:

- пропускной способности каналов связи
- интенсивности трафика, которая может изменяться с течением времени.

Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время, как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

На сетевом уровне определяется два вида протоколов:

- *Определение правил передачи пакетов с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами*. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня.
- *Протокол обмена маршрутной информацией*. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений.

Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

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

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;
- *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, не обремененных многочисленными проверками, квитированием и другими приемами повышения надежности. 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.*

Начиная с транспортного уровня, все вышележащие протоколы реализуются программными средствами, обычно включаемыми в состав сетевой операционной системы. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell.

Сеансовый уровень.

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, *какая из сторон является активной в настоящий момент*, а также *предоставляет средства синхронизации*. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того, чтобы начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Уровень представления.

Этот уровень обеспечивает то, что *информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе*. В случаях 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 такого протокола является протокол

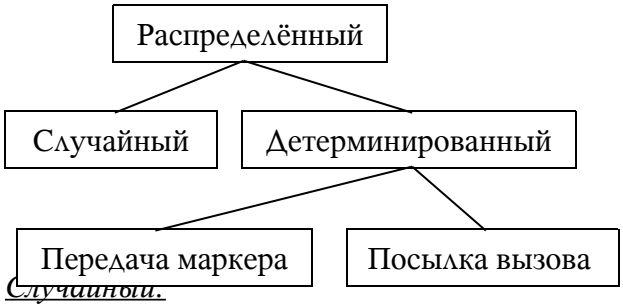
Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

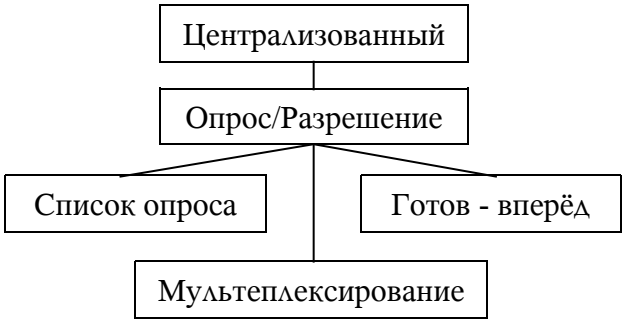
Прикладной уровень.

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

5. Методы доступа к коммуникационной сети (среде)





Случайный:

+ Хороший алгоритм;

+ Возможность широковещательной пердачи;

- Потери из-за коллизий и ожидания доступа.

Детерминированный:

+ Устойчивость к высоким нагрузкам;

+ Возможность несложно реализовать приорететные дисциплины обслуживания;

- Более высокий расход при низких нагрузках;

- Более сложный алгоритм работы.

Централизованный:

+ Легче администрировать;

- Надёжность ниже;

6. Статическое распределение канала в ЛС и региональных сетях

Традиционным способом распределения одного канала — например, телефонного кабеля — между многочисленными конкурирующими пользователями является FDM (Frequency Division Multiplexing — частотное уплотнение). При наличии N пользователей полоса пропускания делится на N диапазонов одинаковой ширины (см. рис. 2.27), и каждому пользователю предоставляется один из них. Поскольку при такой схеме у каждого оказывается свой личный частотный диапазон, то конфликта между пользователями не возникает. При небольшом количестве абонентов, каждому из которых требуется постоянная линия связи (например, коммутаторы операторов связи), частотное уплотнение предоставляет простой и эффективный механизм распределения.

Однако при большом и постоянно меняющемся количестве отправителей данных или пульсирующем трафике частотное уплотнение не может обеспечить достаточно эффективное распределение канала. Если количество пользователей **в** какой-либо момент времени меньше числа диапазонов, на которые разделен спектр частот, то большая часть спектра не используется и тратится попусту. Если, наоборот, количество пользователей окажется больше числа доступных диапазонов, то некоторым придется отказать в доступе к каналу, даже если абоненты, уже захватившие его, почти не будут использовать пропускную способность.

Однако даже если предположить, что количество пользователей можно каким-то способом удерживать на постоянном уровне, то разделение канала на статические подканалы все равно является неэффективным. Основная проблема здесь состоит в том, что если какая-то часть пользователей не пользуется каналом, то эта часть спектра просто пропадает. Они сами при этом занимают линию, не передавая ничего, и другим не дают передать данные. Кроме того, в большинстве компьютерных систем трафик является чрезвычайно неравномерным (вполне обычным является отношение пикового трафика к среднему как 1000:1). Следовательно, большую часть времени большая часть каналов не будет использоваться.

То, что характеристики статического частотного уплотнения оказываются неудачными, можно легко продемонстрировать на примере простых вычислений теории массового обслуживания. Для начала сосчитаем среднее время задержки T для канала с пропускной способностью C бит/с, по которому прибывают λ кадров в секунду. Длина кадров является случайной величиной с экспоненциально распределенной плотностью вероятности, среднее значение которой равно $1/\mu$ бита на кадр. При таких параметрах скорость прибытия составляет λ кадров в секунду, а скорость обслуживания — μC кадров в секунду. Теория массового обслуживания говорит о том, что пуассоновское время прибытия и обслуживания равно

$$T = \frac{1}{\mu C - \lambda}.$$

Пусть, например, пропускная способность C равна 100 Мбит/с, средняя длина кадра $1/\mu$ =10 000 бит, скорость прибытия кадров λ = 5000 кадров в секунду. Тогда T= 200 мкс. Обратите внимание: если бы мы не учли задержки при формировании очереди и просто посчитали, сколько времени нужно на передачу кадра длиной 10 000 бит по сети с пропускной способностью 100 Мбит/с, то получили бы неправильный ответ: 100 мкс. Это число приемлемо лишь при отсутствии борьбы за канал.

Теперь давайте разделим канал на N независимых подканалов, у каждого из которых будет пропускная способность C/N бит/с. Средняя входная скорость в каждом подканале теперь будет равна λ/N кадров в секунду. Сосчитав новое значение средней задержки T, получим:

$$T_{\text{FDM}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT. \qquad (4.1)$$

Это означает, что при использовании частотного уплотнения значение средней задержки стало в N раз хуже значения, которое было бы в канале, если бы все кадры были каким-то волшебным образом организованы в одну общую очередь.

Те же самые аргументы применимы и к временному уплотнению (TDM, Time Division Multiplexing — мультиплексная передача с временным разделением). Каждому пользователю в данном случае статически выделяется N-й интервал времени. Если интервал не используется абонентом, то он просто пропадает. С тем же успехом можно разделить сети физически. Если взять 100-мегабитную сеть и сделать из нее десять 10-мегабитных, статически распределив по ним пользователей, то в результате средняя задержка возрастет с 200 мкс до 2 мс.

Таким образом, ни один статический метод распределения каналов не годится для пульсирующего трафика.

7. Пять допущений в основе динамического распределения каналов.

1.**Станционная модель.** Модель состоит из *N* независимых **станций** (компьютеров, телефонов, персональных средств связи и т. д.), в каждой из которых программа пользователя формирует кадры для передачи. Станции иногда называют терминалами. Вероятность формирования кадра в интервале времени *At* равна *Aλt,* где *λ* является константой (скорость прибытия новых кадров). Как только кадр сформирован, станция блокируется и ничего не делает, пока кадр не будет успешно передан.

2.**Предположение о едином канале.** Единый канал доступен для всех. Все станции могут передавать и принимать данные по нему. С точки зрения аппаратуры все станции считаются равными, хотя программно протокол может устанавливать для них различные приоритеты.

3.**Допущение о коллизиях.** Если два кадра передаются одновременно, они перекрываются по времени, в результате сигнал искажается. Такое событие называется конфликтом, или коллизией. Все станции могут обнаруживать конфликты. Искаженный вследствие конфликта кадр должен быть передан повторно. Других ошибок, кроме тех, которые вызваны конфликтами, нет.

4а. Непрерывное время. Передача кадров может начаться в любой момент времени. Не существует никаких синхронизирующих импульсов, которые делили бы время на дискретные интервалы.

46. Дискретное время. Время разделено на дискретные интервалы (такты). Передача кадра может начаться только с началом такта. Один временной интервал может содержать 0, 1 или более кадров, что соответствует свободному интервалу, успешной передаче кадра или коллизии.

5а. Контроль несущей. Станции могут определить, свободна или занята линия, до ее использования. Если канал занят, станции не будут пытаться передавать кадры по нему, пока он не освободится.

***56.* Отсутствие контроля несущей.** Станции не могут определить, свободна или занята линия, пока не попытаются ее использовать. Они просто начинают передачу. Только потом они могут определить, была ли передача успешной.

Первое допущение утверждает, что станции независимы и работают с постоянной скоростью. Также неявно предполагается, что у каждой станции имеется только один пользователь или программа, поэтому пока станция заблокирована, она не производит никакой работы. Более сложные модели рассматривают

многопрограммные станции, которые могут работать в заблокированном состоянии, однако и анализ подобных станций намного сложнее.

Допущение о едином канале является, на самом деле, центральным в данной модели. Никаких внешних каналов связи нет.

Допущение о коллизиях также является основным, хотя в некоторых системах (особенно в системах с расширенным спектром) данное допущение звучит не столь строго, что приводит к неожиданным результатам. Кроме того, в некоторых локальных сетях, например в сети *token ring* (маркерное кольцо), применяется механизм разрешения коллизий, реализуемый за счет специальных пакетов — маркеров, передающихся от станции к станции. Помещать в канал кадр может только тот, у кого в данный момент находится маркер. Далее мы обсудим модель моноканала с конкуренцией и коллизиями.

Для времени существует два альтернативных допущения. В одних системах время может быть непрерывным *(4а),* в других — дискретным, поэтому мы рассмотрим оба варианта.

Аналогично этому, контроль несущей также реализован не во всех системах. Станции локальных сетей обычно знают, когда линия занята, однако в беспроводных сетях контроля несущей нет, потому что отдельно взятая станция не может «слышать» все остальные из-за разницы частотных диапазонов. Станции проводных сетей с контролем несущей могут приостанавливать собственную передачу, обнаружив коллизию. Обратите внимание на слово «несущая». В данном случае оно означает электрический сигнал, распространяющийся по каналу.

8. Протокол коллективного доступа в системе чистая ALOHA

В основе системы ALOHA лежит простая идея: разрешить пользователям передачу, как только у них появляются данные для отсылки. Конечно, при этом будут столкновения, и столкнувшиеся кадры будут разрушены. Однако благодаря свойству обратной связи широковещательной системы отправитель всегда может установить, дошел ли его кадр до получателя или был разрушен. Для этого ему нужно просто прослушивать канал, как это делают все остальные пользователи. В локальных сетях обратная связь мгновенная, а в спутниковых системах существует задержка в 270 мс, и только после этого отправитель может узнать, насколько успешной была передача. Если кадр был уничтожен, отправитель просто выжидает некоторое случайное время и пытается переслать этот кадр снова. Время ожидания должно быть случайным. В противном случае при равных фиксированных интервалах времени ожидания коллизии будут повторяться снова и снова. Системы, в которых несколько пользователей используют один общий канал таким способом, что время от времени возникают конфликты, называются системами с конкуренцией.

На рис. 4.1 показан пример формирования кадров в системе ALOHA. Все кадры на нашем рисунке имеют один размер, так как при этом пропускная способность системы сделана максимальной именно за счет фиксированного размера кадров.

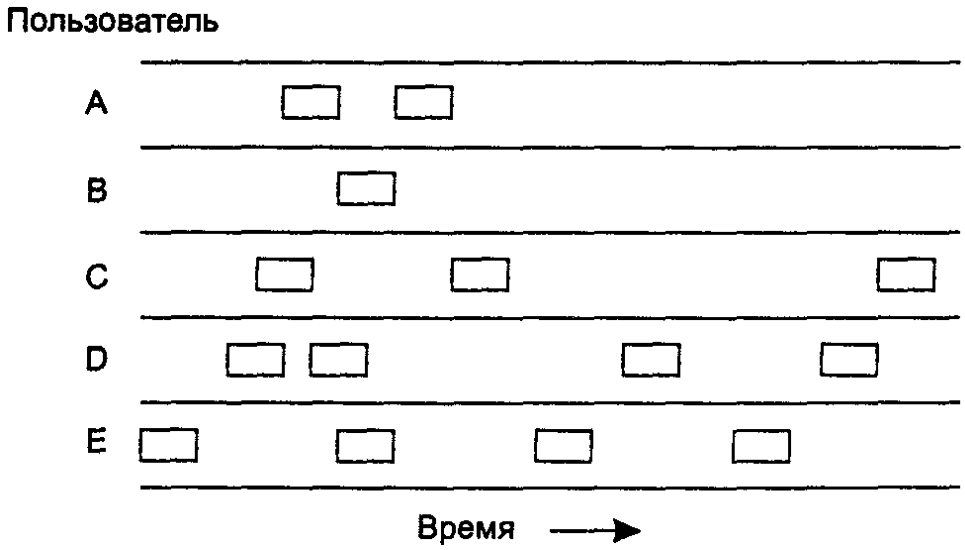


Рис. 4.1. В чистой системе ALOHA кадры передаются в абсолютно произвольное время

Когда два кадра одновременно пытаются занять канал, они сталкиваются и уничтожаются. Даже если только один первый бит второго кадра перекрывается последним битом первого кадра, оба кадра уничтожаются полностью. При этом оба кадра будут переданы позднее повторно. Контрольная сумма не может (и не должна) отличать полную потерю информации от частичной. Потеря есть потеря.

Самым интересным в данной ситуации является вопрос об эффективности канала системы ALOHA. Другими словами, какая часть всех передаваемых кадров способна избежать коллизий при любых обстоятельствах? Сначала рассмотрим бесконечное множество интерактивных пользователей, сидящих за своими компьютерами (станциями). Пользователь всегда находится в одном из двух состояний: ввод с клавиатуры и ожидание. Вначале все пользователи находятся в состоянии ввода. Закончив набор строки, пользователь перестает вводить текст, ожидая ответа. В это время станция передает кадр, содержащий набранную строку, и опрашивает канал, проверяя успешность передачи кадра. Если кадр передан успешно, пользователь видит ответ и продолжает набор. В противном случае пользователь ждет, пока кадр не будет передан.

Пусть «время кадра» означает интервал времени, требующийся для передачи стандартного кадра фиксированной длины (то есть длину кадра, деленную на скорость передачи данных). На данный момент мы предполагаем, что бесконечное количество пользователей порождает новые кадры, распределенные по Пуассону со следующим средним значением: N кадров за время кадра. (Допущение о бесконечном количестве пользователей необходимо для того, чтобы гарантировать, что величина N не станет уменьшаться по мере блокирования пользователей.) Если $N > 1$, это означает, что сообщество пользователей формирует кадры с большей скоростью, чем может быть передано по каналу, и почти каждый кадр будет страдать от столкновений. Мы будем предполагать, что $0 < N < 1$.

Помимо новых кадров, станции формируют повторные передачи кадров, пострадавших от столкновений. Допустим также, что вероятность k попыток передачи старых и новых кадров за время кадра также имеет пуассоновское распределение со средним значением G за время кадра. Очевидно, что $G > N$. При малой загрузке канала (то есть при $N \approx 0$) столкновений будет мало, поэтому мало будет и повторных передач, то есть $G \approx N$. При большой загрузке канала столкновений будет много, а следовательно, $G > N$. Какая бы ни была нагрузка, производительность канала S будет равна предлагаемой загрузке G, умноженной на вероятность успешной передачи, то есть $S = GP_0$, где P_o — вероятность того, что кадр не пострадает в результате коллизии.

Кадр не пострадает от коллизии в том случае, если в течение интервала времени его передачи не будет послано больше ни одного кадра, как показано на рис. 4.2. При каких условиях затененный кадр будет передан без повреждений? Пусть t — это время, требуемое для передачи кадра. Если какой-либо

пользователь сформирует кадр в интервале времени между t_0 и $t_0 + t$, то конец этого кадра столкнется с началом затененного кадра. При этом судьба затененного кадра предрешена еще до того, как будет послан его первый бит, однако, поскольку в чистой системе ALOHA станции не прослушивают канал до начала передачи, у них нет способа узнать, что канал занят и по нему уже передается кадр. Аналогичным образом любой другой кадр, передача которого начнется в интервале от $t_0 + t$ до $t_0 + 2t$, столкнется с концом затененного кадра.

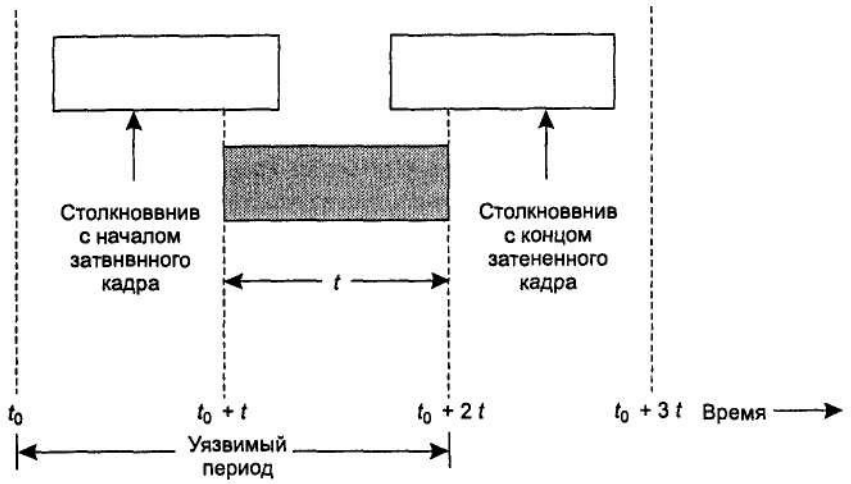


Рис. 4.2. Опасный интервал времени для затененного кадра

Вероятность того, что в течение времени кадра будет сформировано k кадров, можно вычислить по формуле распределения Пуассона:

$$\Pr[k] = \frac{G^k e^{-G}}{k!}.$$

Таким образом, вероятность формирования нуля кадров в течение этого интервала времени равна e^{-G}. Среднее количество кадров, сформированных за интервал времени длиной в два кадра, равно $2G$. Вероятность того, что никто не начнет передачу в течение всего опасного периода, равна $P_0 = e^{-2G}$. Учитывая, что $S = GP_0$, получаем:

$$S = Ge^{-2G}.$$

Зависимость производительности канала от предлагаемого трафика показана на рис. 4.3. Максимальная производительность достигает значения S = 1/2e, что приблизительно равно 0,184 при G = 0,5. Другими словами, лучшее, на что мы можем надеяться, — это использовать канал на 18 %. Этот результат несколько разочаровывает, однако в случае, когда каждый передает, когда хочет, трудно ожидать стопроцентного успеха.

9. Протокол коллективного доступа в системе дискретная ALOHA

В 1972 г. Роберте (Roberts) опубликовал описание метода, позволяющего удвоить производительность систем ALOHA (Roberts, 1972). Его предложение заключалось в разделении времени на дискретные интервалы, соответствующие времени одного кадра. При таком подходе пользователи должны согласиться с определенными временными ограничениями. Одним из способов достижения

синхронизации является установка специальной станции, испускающей синхронизирующий сигнал в начале каждого интервала.

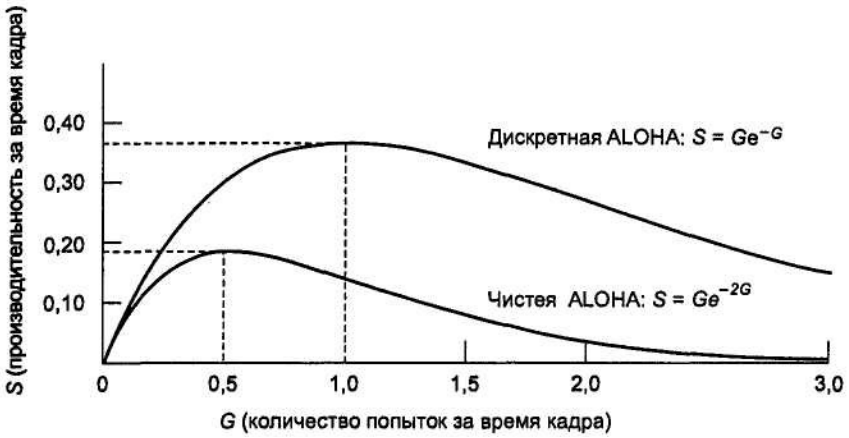


Рис. 4.3. Зависимость производительности канала от предлагаемого трафика для систем ALOHA

В системе Робертса, известной под названием **дискретная ALOHA,** в отличие **от чистой системы ALOHA** Абрамсона, компьютер не может начинать передачу сразу после нажатия пользователем клавиши Enter. Вместо этого он должен дождаться начала нового такта. Таким образом, непрерывная чистая система ALOHA превращается в дискретную. Поскольку опасный временной интервал теперь становится в два раза короче, вероятность отсутствия передачи по каналу за тот же интервал времени, в течение которого передается тестовый кадр, равна e^{-G}. В результате получаем:

$$S = Ge^{-G}. \qquad (4.3)$$

Как видно из рис. 4.3, дискретная система ALOHA имеет пик при $G = 1$. При этом производительность канала составляет $S = 1/e$, что приблизительно равно 0,368, то есть в два раза больше, чем в чистой системе ALOHA. Для дискретной системы ALOHA в оптимальной ситуации 37 % интервалов будут пустыми, 37 % — с успешно переданными кадрами и 26 % — со столкнувшимися кадрами. При увеличении количества попыток передачи в единицу времени G количество пустых интервалов уменьшается, но увеличивается количество конфликтных интервалов. Чтобы увидеть, насколько быстро растет количество конфликтных интервалов, рассмотрим передачу тестового кадра.

Вероятность того, что он избежит столкновения, равна e^{-G}. Фактически, это вероятность того, что все остальные пользователи будут молчать в течение данного тактового интервала. Таким образом, вероятность столкновения равна 1 - e^{-G}. Вероятность передачи кадра ровно за *k попыток (то есть после k - 1 столкновения, за которыми последует успешная передача), равна*

$$P_k = e^{-G}(1 - e^{-G})^{k-1}.$$

Ожидаемое число попыток передачи для одного кадра равно

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1 - e^{-G})^{k-1} = e^{G}.$$

Поскольку число попыток передачи для одного кадра *E* экспоненциально зависит от количества попыток передачи в единицу времени *G,* небольшое увеличение нагрузки в канале может сильно снизить его производительность.

Дискретная система ALOHA чрезвычайно важна по одной причине, которая на первый взгляд не кажется очевидной. Она появилась в 1970-х годах, применялась в некоторых экспериментальных системах, затем была почти забыта. Когда был изобретен метод доступа в Интернет по кабельным сетям, вновь возникла проблема распределения единственного канала между большим числом конкурирующих абонентов. Тогда с полок достали запыленные описания дискретной ALOHA.

10. Протоколы множественного доступа с контролем несущей

В дискретной системе ALOHA максимальный коэффициент использования канала, который может быть достигнут, равен 1/e. Такой результат неудивителен, поскольку станции передают данные, когда хотят, не считаясь с тем, что делают остальные станции. В такой системе неизбежно возникает большое количество коллизий. Однако в локальных сетях можно организовать процесс таким образом, что станции будут учитывать поведение друг друга. За счет этого можно достичь значения коэффициента использования канала значительно большего, чем 1/e.

Протоколы, в которых станции прослушивают среду передачи данных и действуют в соответствии с этим, называются протоколами с контролем несущей.

Настойчивый и ненастойчивый CSMA

Первый протокол с опросом несущей, который мы рассмотрим, называется **1-на-стойчивый протокол CSMA** (Carrier Sense Multiple Access — множественный доступ с контролем несущей). Когда у станции появляются данные для передачи, она сначала прослушивает канал, проверяя, свободен он или занят. Если канал занят, то есть по нему передает какая-либо другая станция, станция ждет, пока он освободится. Когда канал освобождается, станция передает кадр. Если происходит столкновение, станция ждет в течение случайного интервала времени, затем снова прослушивает канал и, если он свободен, пытается передать кадр еще раз. Такой протокол называется *протоколом CSMA с настойчивостью 1*, так как станция передает кадр с вероятностью 1, как только обнаружит, что канал свободен.

Задержка распространения сигнала оказывает сильное влияние на производительность данного протокола. Существует небольшая вероятность того, что как только станция начнет передачу, другая станция также окажется готовой к передаче и опросит канал. Если сигнал от первой станции еще не успел достичь второй станции, вторая станция решит, что канал свободен, и также начнет передачу,

результатом чего будет коллизия. Чем больше время распространения сигнала, тем выше вероятность столкновений и ниже производительность протокола.

Даже при нулевой задержке распространения сигнала все равно будут столкновения. Производительность системы с опросом несущей должна быть выше даже чем у дискретной системы ALOHA.

Вторым протоколом с опросом несущей является ***ненастойчивый протокол CSMA***. В данном протоколе предпринята попытка сдержать стремление станций начинать передачу, как только освобождается канал. Прежде чем начать передачу, станция опрашивает канал. Если никто не передает в данный момент по каналу, станция начинает передачу сама. Однако если канал занят, станция не ждет освобождения канала, постоянно прослушивая его и пытаясь захватить сразу, как только он освободится, как в предыдущем протоколе. Вместо этого станция ждет в течение случайного интервала времени, а затем снова прослушивает линию. Очевидно, данный алгоритм должен привести к лучшему использованию канала и к большим интервалам ожидания, чем протокол CSMA с настойчивостью 1.

Третий протокол, это ***протокол CSMA с настойчивостью p***. Он применяется в дискретных каналах и работает следующим образом. Когда станция готова передавать, она опрашивает канал. Если канал свободен, она с вероятностью p начинает передачу. С вероятностью $q = 1 - p$ она отказывается от передачи и ждет начала следующего такта. Этот процесс повторяется до тех пор, пока кадр не будет передан или какая-либо другая станция не начнет передачу. В последнем случае станция ведет себя так же, как в случае столкновения. Она ждет в течение случайного интервала времени, после чего начинает все снова. Если при первом прослушивании канала он оказывается занят, станция ждет следующего интервала времени, после чего применяется тот же алгоритм.

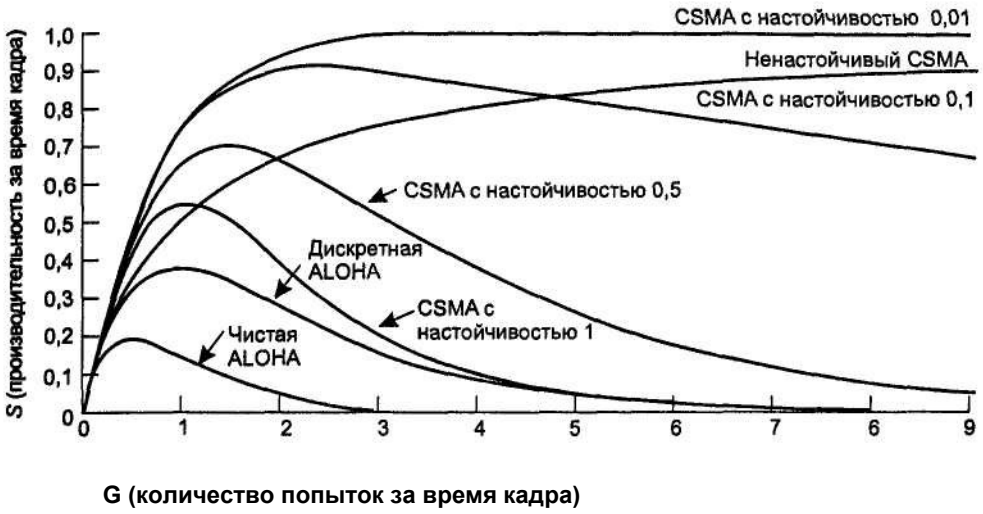


Рис. 4.4. Сравнение использования канала в зависимости от его загрузки для различных протоколов коллективного доступа

/* Протокол CSMA с обнаружением конфликтов

Настойчивый и ненастойчивый протоколы CSMA, несомненно, являются улучшениями системы ALOHA, поскольку они гарантируют, что никакая станция не начнет передачу, если она определит, что канал уже занят. Еще одним шагом вперед является прекращение станцией передачи, если выясняется, что произошел конфликт. Другими словами, если две станции, обнаружив, что канал свободен, одновременно начали передачу, они практически немедленно обнаруживают столкновение. Вместо того чтобы пытаться продолжать передачу своих кадров, которые все равно уже не могут быть приняты получателями, им следует прекратить передачу. Таким образом экономится время и улучшается производительность канала. Такой протокол, называемый CSMA/CD (Carrier-Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов), широко

применяется в локальных сетях в подуровне MAC. В частности, он является основой чрезвычайно популярных ЛВС Ethernet, поэтому мы уделим некоторое время более или менее подробному рассмотрению CSMA/CD.

В протоколе CSMA/CD, так же как и во многих других протоколах локальных сетей, применяется концептуальная модель, показанная на рис. 4.5. В момент времени t_Q одна из станций закончила передачу кадра. Все остальные станции, готовые к передаче, теперь могут попытаться передать свои кадры. Если две или более станций одновременно начнут передачу, то произойдет столкновение. Столкновения могут быть обнаружены по мощности или длительности импульса принимаемого сигнала в сравнении с передаваемым сигналом.

Обнаружив коллизию, станция прекращает передачу, ждет случайный период времени, после чего пытается снова при условии, что к этому моменту не начала передачу другая станция. Таким образом, наша модель протокола CSMA/CD будет состоять из чередования периодов конкуренции и передачи, а также периодов простоя канала (когда все станции молчат).

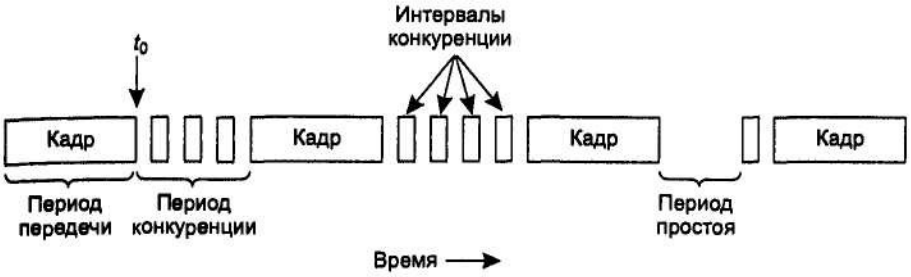


Рис. 4.5. Протокол CSMA/CD может находиться в одном из трех состояний: конкуренции, передачи и простоя

Рассмотрим более подробно алгоритм борьбы за право передачи по каналу. Предположим, две станции одновременно начали передачу в момент времени t_0. Сколько понадобится времени на то, чтобы они поняли, что произошло столкновение? От ответа на этот вопрос зависит длина периода конкуренции, а следовательно, величина задержки и производительность канала. Минимальное время обнаружения конфликта равно времени распространения сигнала от одной станции до другой.

Исходя из этих рассуждений, можно предположить, что станция, которая не слышит столкновения в течение времени, требующегося для прохождения сигнала по всему кабелю, может быть уверена, что ей удалось захватить кабель. Под термином «захватить» имеется в виду, что все остальные станции знают, что эта станция передает, и не будут сами пытаться передавать. Однако такое заключение неверно. Рассмотрим следующий сценарий. Пусть время, необходимое для прохождения сигнала между двумя самыми дальними станциями, равно т. В момент времени t_0 одна из станций начинает передачу. Через интервал времени т - (епсилон), за мгновение до того, как сигнал достигнет самой дальней станции, та станция также начинает передавать. Конечно, почти мгновенно она обнаруживает столкновение и останавливается, но всплеск шума, вызванный столкновением, достигает передающей станции только через интервал времени 2т - (эпсилон) с момента начала передачи. Другими словами, станция не может быть уверена в том, что захватила канал, до тех пор, пока не пройдет интервал времени 2т с момента начала передачи. По этой причине для моделирования интервала конкуренции мы будем использовать дискретную систему ALOHA с шириной интервала 2т. В коаксиальном кабеле длиной 1 км (тау) (примерно равно) 5 мкс. Для простоты мы будем предполагать, что каждый интервал времени 2т содержит всего 1 бит. Как только канал захвачен, станция может передавать с любой скоростью, не обязательно 1 бит за 2т с.

Следует отметить, что обнаружение столкновения является *аналоговым* процессом. Аппаратура станции должна прослушивать кабель во время передачи. При этом, если то, что она слышит, отличается от того, что она передает, станция понимает, что произошло столкновение. Способ кодирования сигнала

должен позволять определять столкновения (например, столкновение двух сигналов в 0 В в явном виде не так просто обнаружить). По этой причине используется специальное кодирование.

Передающая станция должна постоянно прослушивать канал, выявляя всплески шума, которые могут означать столкновение. По этой причине CSMA/CD с моноканалом считается полудуплексной системой. Станция не может одновременно передавать и принимать кадры, поскольку задействован механизм обратной связи для определения столкновений.

Во избежание неправильного понимания вопроса следует также отметить, что ни один протокол подуровня MAC не может гарантировать надежную доставку. Даже при отсутствии столкновений получатель может не получить правильную копию кадра по различным причинам (например, из-за нехватки места в буфере или пропущенного прерывания). */

11. Протоколы множественного доступа без столкновений

В описываемых далее протоколах предполагается наличие N станций, у каждой из которых есть постоянный уникальный адрес в пределах от 0 до *N*- 1. То, что некоторые станции могут часть времени оставаться пассивными, роли не играет. Также предполагается, что задержка распространения сигнала пренебрежимо мала. Главный вопрос сохраняется: какой станции будет предоставлен канал после передачи данного кадра? Будем использовать модель, изображенную на рис. 4.5, с ее дискретными интервалами конкуренции.

Протокол битовой карты

В первом протоколе без столкновений, называющемся **основным методом битовой карты,** каждый период конкуренции состоит ровно из N временных интервалов. Если у станции 0 есть кадр для передачи, она передает единичный бит во время 0-го интервала. Другим станциям не разрешается передача в это время. Во время интервала 1 станция 1 также сообщает, есть ли у нее кадр для передачи, передавая бит 1 или 0. В результате к окончанию интервала N все N станций знают, кто хочет передавать. В этот момент они начинают передачу в соответствии со своим порядком номеров (рис. 4.6).

Поскольку все знают, чья очередь передавать, столкновений нет. После того как последняя станция передает свой кадр, что все станции отслеживают, прослушивая линию, начинается новый период подачи заявок из N интервалов. Если станция переходит в состояние готовности (получает кадр для передачи) сразу после того, как она отказалась от передачи, это значит, что ей не повезло и она **должна** ждать следующего цикла. Протоколы, в которых намерение передавать **объявляется** всем перед самой передачей, называются **протоколами** с **резервированием.**

Рис. 4.6. Базовый протокол битовой карты

Оценим производительность такого протокола. Для удобства будем измерять время в однобитовых интервалах периода подачи заявок, при этом кадр данных состоит из d единиц времени. При слабой загрузке канала бит-карта просто будет повторяться снова и снова, изредка перемежаясь кадрами.

Рассмотрим эту ситуацию с точки зрения станции с небольшим номером, например, 0 или 1. Обычно в тот момент, когда у нее возникает потребность в передаче, текущий интервал времени уже находится где-то в середине бит-карты. В среднем станция будет ждать $N/2$ интервалов до окончания текущего периода резервирования и еще N интервалов следующего (своего) периода резервирования, не считая кадров, передаваемых между двумя этими периодами, прежде чем она сможет начать передачу.

Перспективы станций с большими номерами более радужны. В среднем время ожидания передачи составит половину цикла ($N/2$ однобитовых интервалов). Станциям с большими номерами редко приходится ждать следующего цикла. Поскольку станциям с небольшими номерами приходится ждать в среднем $1{,}5N$ интервалов, а станциям с большими номерами — N/2 интервалов, среднее время ожидания для всех станций составляет N интервалов. При низкой загрузке канала его производительность легко сосчитать. Накладные расходы на кадр составляют N бит, и при длине кадра в d бит эффективность равна $d/(N + d)$.

При сильной загруженности канала, когда все станции хотят что-то передать, период подачи заявок из N *бит* чередуется с N кадрами. При этом накладные расходы на передачу одного кадра составляют всего один бит, а эффективность равна $d/(d+1)$. Среднее время задержки для кадра будет равно сумме времени ожидания в очереди внутри своей станции и дополнительных $N(d + 1)/2$ однобитовых интервалов, когда он попадет в начало своей внутренней очереди.

Двоичный обратный отсчет

Недостатком базового протокола бит-карты являются накладные расходы в 1 бит на станцию. Используя двоичный адрес станции, можно улучшить эффективность канала. Станция, желающая занять канал, объявляет свой адрес в виде битовой строки, начиная со старшего бита. Предполагается, что все адреса станций имеют одинаковую длину. Биты адреса в каждой позиции логически складываются (логическое ИЛИ). Мы будем называть этот протокол протоколом с двоичным обратным отсчетом. Неявно предполагается, что задержки распространения сигнала пренебрежимо малы, поэтому станции слышат утверждаемые номера практически мгновенно.

Во избежание конфликтов следует применить правило арбитража: как только станция с 0 в старшем бите адреса видит, что в суммарном адресе этот 0 заменился единицей, она сдается и ждет следующего цикла. Например, если станции 0010, 0100, 1001 и 1010 конкурируют за канал, то в первом битовом интервале они передают биты 0, 0, 1 и 1 соответственно. В этом случае суммарный первый бит адреса будет равен 1. Следовательно, станции с номерами 0010 и 0100 считаются проигравшими, а станции 1001 и 1010 продолжают борьбу.

Следующий бит у обеих оставшихся станций равен 0 — таким образом, обе продолжают. Третий бит равен 1, поэтому станция 1001 сдается. Победителем оказывается станция 1010, так как ее адрес наибольший. Выиграв торги, она может начать передачу кадра, после чего начнется новый цикл торгов. Схема протокола показана на рис. 4.7. Данный метод предполагает, что приоритет станции напрямую зависит от ее номера. В некоторых случаях такое жесткое правило может играть положительную, в некоторых — отрицательную роль.

Рис. 4.7. Протокол с двоичным обратным отсчетом. Прочерк означает молчание

Эффективность использования канала при этом методе составляет $d/(d + \log_2 N)$. Однако можно так хитро выбрать формат кадра, что его первое поле будет содержать адрес отправителя, тогда даже эти $\log_2 N$ бит не пропадут зря и эффективность составит 100 %.

Мок (Мок) и Уард (Ward) в 1979 году описали вариант протокола с обратным отсчетом, в котором использовался параллельный, а не последовательный интерфейс. Они также предложили использовать виртуальные номера станций. После каждой передачи станции, которая успешно послала кадр, присваивается виртуальный номер 0, тем самым дается возможность захвата канала станциями, которые молчат слишком долго. Например, если станции С, Н, *D, A, G, B, E, F* имели приоритеты 7, 6, 5, 4, 3, 2, 1 и 0 соответственно, тогда при успешной передаче станции *D* она помещается в конец списка, получая номер 0. Приоритеты старших станций *C* и *H* остаются неизменными (7 и 6), а приоритеты остальных станций увеличиваются на 1 (например, приоритет А был 4, а стал 5). Таким образом, на следующем цикле формируется такой список: *C, H, A, G, B, E, F, D.* Теперь станция *D* сможет получить доступ к каналу, только если он больше никому не нужен.

/*Протоколы с ограниченной конкуренцией

Итак, мы рассмотрели две основные стратегии предоставления доступа к каналу в кабельных сетях: соревнование, как в CSMA, и бесконфликтные методы. Каждую стратегию можно оценить по двум важным параметрам: времени задержки при низкой загрузке канала и эффективности канала при большой загрузке. В условиях низкой загрузки конфликты (то есть чистая или дискретная системы ALOHA) предпочтительнее, так как время задержки в таких системах меньше. По мере роста загруженности канала системы со столкновениями становятся все менее привлекательными, поскольку возрастают накладные расходы, связанные с конфликтами. Для бесконфликтных протоколов справедливо обратное. При низкой нагрузке у них довольно высокое время задержки, но по мере увеличения нагрузки эффективность использования канала не уменьшается, как у конфликтных протоколов, а наоборот, возрастает.

Очевидно, было бы неплохо объединить лучшие свойства обеих стратегий и получить протокол, использующий разные стратегии при разной загруженности канала. Такие протоколы мы будем называть протоколами с ограниченной конкуренцией. Они в самом деле существуют, и их рассмотрением мы завершим изучение сетей с опросом носителя.

До сих пор мы рассматривали только симметричные протоколы коллективного доступа, в которых каждая станция пытается получить доступ к каналу с равной вероятностью *p*. Интересно, что производительность всей системы может быть улучшена при использовании асимметричного протокола, в котором станциям назначаются различные вероятности.

Прежде чем приступить к рассмотрению асимметричных протоколов, давайте кратко рассмотрим производительность в симметричном случае. Предположим, что *k* станций борются за доступ к каналу. Вероятность передачи каждой станции в каждый интервал времени равна *p*. Вероятность того, что какая-то станция успешно получит доступ к каналу на данный интервал времени, равна *kp(l - p)^(k-1)*-Чтобы найти оптимальное значение вероятности *p,* продифференцируем данное выражение по *p,* приравняем результат к нулю и решим полученное уравнение относительно *p*. В результате мы получим, что наилучшее значение *p* равно *1/k*. Заменяя в формуле *p* на *1/k,* получаем вероятность успеха при оптимальном значении *p:*

P[успех при оптимальной вероятности p $= \left(\frac{k-1}{k}\right)^{k-1}$.

Разработчикам Ethernet удалось добиться хороших показателей по самым главным направлениям. Скорости выросли на несколько порядков, в систему были внедрены коммутаторы и хабы, но эти изменения никак не коснулись программного обеспечения. Если продавец скажет: «Вот отличная новая сетевая система! Она работает просто фантастически быстро и надежно! Вам необходимо только выкинуть весь ваш старый железный хлам и стереть все старые программы», — у него возникнут проблемы с объемами продаж. FDDI, волоконно-оптический канал и ATM были, конечно, быстры, ничего не скажешь, особенно по сравнению с тогдашним Ethernet, но именно из-за того, что они не были совместимы с Ethernet и были гораздо сложнее и тяжелее в обслуживании, про них вскоре все забыли. А потом оказалось, что Ethernet догнал и перегнал их по скорости работы, сумев не растерять при этом все свои старые достоинства. Все соперники Ethernet давно почили в бозе, кроме ATM, — этакой телефонной крысы, живущей в самом ядре телефонии. */

12. Модели архитектур локальных сетей

13. Методы адресации в сетях

Существуют различные схемы адресации, используемые определение местонахождения компьютерных систем, которые зависят от используемого семейства протоколов. Другими словами, адресация AppleTalk отличается от адресации TCP/IP, которая в свою очередь отличается от адресации OSI, и т.д.

<u>Два типа адресов:</u>

- адреса канального уровня;
- адреса сетевого уровня.

Адреса канального уровня (называемые также физическими или аппаратными адресами), как правило, уникальны для каждого сетевого соединения. У большинства локальных сетей (LAN) адреса канального уровня *размещены в схеме интерфейса*; они назначаются той организацией, которая определяет стандарт протокола, представленный этим интерфейсом. Т.к. большинство компьютерных систем имеют одно физическое сетевое соединение, они имеют только один адрес канального уровня. Роутеры и другие системы, соединенные с множеством физических сетей, могут иметь множество адресов канального уровня. В соответствии с названием, адреса канального уровня существуют на Уровне 2 эталонной модели ISO.

Адреса сетевого уровня (называемые также виртуальными или логическими адресами) существуют на Уровне 3 эталонной модели OSI. В отличие от адресов канального уровня, которые обычно существуют в пределах плоского адресного пространства, адреса сетевого уровня обычно иерархические. Другими словами, они похожи на почтовые адреса, которые описывают местонахождение человека, указывая страну, штат, почтовый индекс, город, улицу, адрес на этой улице и, наконец, имя. Хорошим примером одноуровневой адресации является номерная система социальной безопасности США, в соответствии с которой каждый человек имеет один уникальный номер, присвоенный ему службой безопасности.

Иерархические адреса делают сортировку адресов и повторный вызов более легкими путем исключения крупных блоков логически схожих адресов в процессе последовательности операций сравнения. Например, можно исключить все другие страны, если в адресе указана страна "Ирландия". Легкость сортировки и повторного вызова являются причиной того, что роутеры используют адреса сетевого уровня в качестве базиса маршрутизации.

Адреса сетевого уровня различаются в зависимости от используемого семейства протоколов, однако они, как правило, *используют соответствующие логические разделы для нахождения компьютерных систем в объединенной сети*. Некоторые из этих логических разделов базируются на физических характеристиках сети (таких, как сегмент сети, в котором находится какая-нибудь система); другие логические разделы базируются на группировках, не имеющих физического базиса (например, "зона" AppleTalk).

14. Характеристики сетевых систем

Выделяют две группы характеристик:

- одна группа характеризует *производительность* сети,
- вторая группа характеризует *надежность* сети.

Производительность измеряется с помощью показателей двух типов:

- *Временных,* оценивающих задержку**,** вносимую сетью при выполнении обмена данными;
- Показателей *пропускной способности,* отражающих количество информации, переданной сетью в единицу времени.

- *Время реакции*. Определяется как интервал времени между возникновением запроса пользователя к серверу и получением ответа на этот запрос (рис. 1.5). Смысл и значение этого показателя зависят от типа сервиса, к которому обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния других элементов сети - загруженности сегментов, через которые проходит запрос, загруженности сервера, коммутатора, моста, маршрутизатора и т.п.

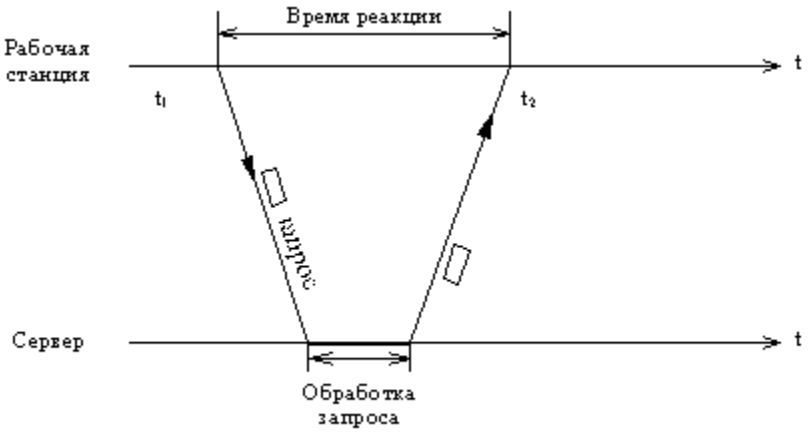


Рис. 1.5. Время реакции - интервал между запросом и ответом

Маршрут (путь) доставки сообщения (обмена сообщениями) может включать какое либо сочетание устройств. Каждое из них вносит определенную задержку. Задержки суммируются и определяют время реакции.

Вариантами этого критерия могут служить времена реакции, измеренные при различных, но фиксированных состояниях сети (крайние значения):

a) ***Полностью ненагруженная сеть.*** Время реакции измеряется в условиях, когда к серверу обращается только один клиент, то есть на сегменте сети, объединяющем сервер с клиентом, нет никакой другой активности. Явление экзотическое. Данный вариант показателя производительности имеет ограниченную применимость - его хорошие значения говорят только о том, что программное обеспечение и аппаратура данных двух узлов и сегмента обладают необходимой производительностью для работы в облегченных условиях.
b) ***Нагруженная сеть.*** Сложности - трафик в сети носит пульсирующий характер, и характеристики трафика существенно изменяются в зависимости от времени дня и дня недели, то определение типовой нагрузки - процедура сложная, требующая длительных измерений на сети. Если же сеть только проектируется, то определение типовой нагрузки еще больше усложняется.

При оценке производительности сети по отношению ко всем узлам в целом используются критерии двух типов: *средневзвешенные* и *пороговые*.

Средневзвешенный критерий представляет собой сумму времен реакции узлов при взаимодействии со всеми или некоторыми серверами сети по определенному сервису, то есть сумму вида

$$(\Sigma_i \Sigma_j T_{ij})/(n \times m)$$

где T_{ij} - время реакции i-го клиента при обращении к j-му серверу, n - число клиентов, m - число серверов.

Пороговый критерий отражает наихудшее время реакции по всем возможным сочетаниям клиентов, серверов и сервисов:

$$\max_{ijk} T_{ijk},$$

где i и j имеют тот же смысл, что и в предыдущем случае, а k обозначает тип сервиса.

Чаще применяются пороговые критерии оптимизации, так как они гарантируют всем пользователям некоторый удовлетворительный уровень реакции сети на их запросы. Средневзвешенные критерии могут дискриминировать некоторых пользователей, для которых время реакции слишком велико при том, что при усреднении получен вполне приемлемый результат.

Информационный кадр, пакет имеют накладные расходы (служебные поля). Эффективная скорость передачи всегда меньше номинальной.

Показатели надежности и отказоустойчивости

Надежность - способность правильно функционировать в течение продолжительного периода времени. Это свойство имеет три составляющих:

- надежность;

- готовность;
- удобство обслуживания.

Надежность измеряется *интенсивностью отказов* и *средним временем наработки на отказ*. Надежность сетей как распределенных систем во многом определяется надежностью кабельных систем и коммутационной аппаратуры - разъемов, кроссовых панелей, коммутационных шкафов и т.п., обеспечивающих собственно электрическую или оптическую связность отдельных узлов между собой.

Критерием оценки готовности является *коэффициент готовности*, который равен доле времени пребывания системы в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии. Коэффициент готовности вычисляется как отношение среднего времени наработки на отказ к сумме этой же величины и среднего времени восстановления. Системы с высокой готовностью называют также ***отказоустойчивыми***.

Основным способом повышения готовности является *избыточность*, на основе которой реализуются различные варианты отказоустойчивых архитектур. Если рассматривать сеть только как транспортную систему, то избыточность должна существовать для всех магистральных маршрутов сети, то есть маршрутов, являющихся общими для большого количества клиентов сети. Такими маршрутами обычно являются маршруты к корпоративным серверам - серверам баз данных, Web-серверам, почтовым серверам и т.п.

Высокую степень готовности сети можно обеспечить в том случае, когда процедуры тестирования работоспособности элементов сети и перехода на резервные элементы встроены в коммуникационные протоколы. Существуют специальные протоколы, поддерживающие отказоустойчивость сети, например, протокол SpanningTree, выполняющий автоматический переход на резервные связи в сети, построенной на основе мостов и коммутаторов.

Между показателями производительности и надежности сети существует тесная связь. Ненадежная работа сети очень часто приводит к существенному снижению ее производительности. Это объясняется тем, что сбои и отказы каналов связи и коммуникационного оборудования приводят к потере или искажению некоторой части пакетов, в результате чего коммуникационные протоколы вынуждены организовывать повторную передачу утерянных данных. Так как в локальных сетях восстановлением утерянных данных занимаются как правило протоколы транспортного или прикладного уровня, работающие с тайм-аутами в несколько десятков секунд, то потери производительности из-за низкой надежности сети могут составлять сотни процентов.

15. Базовые технологии локальных сетей

Стандарты технологии Ethernet

Ethernet – это самый распространенный на сегодняшний день стандарт локальных сетей. Общее количество сетей, использующих в настоящее время Ethernet, оценивается в более 5 миллионов.

Ethernet – это сетевой стандарт. Использовались различные варианты случайного доступа к общей радиосреде, получившие название Aloha. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля.

На основе этого стандарта Ethernet был разработан стандарт IEEE 802.3, который во многом совпадает со своим предшественником, но некоторые различия все же имеются. В то время, как в стандарте IEEE 802.3 различаются уровни MAC и LLC, в оригинальном Ethernet оба эти уровня объединены в единый канальный уровень. В Ethernet определяется протокол тестирования конфигурации (Ethernet Configuration

Test Protocol), который отсутствует в IEEE 802.3. Несколько отличается и формат кадра, хотя минимальные и максимальные размеры кадров в этих стандартах совпадают.

Для передачи двоичной информации по кабелю для всех вариантов физического уровня технологии Ethernet используется манчестерский код.

Все виды стандартов Ethernet используют один и тот же метод разделения среды передачи данных - метод CSMA/CD (carrier sense multiply access/collision detection – контроль несущей множественный доступ/обнаружение столкновений).

Топология – шина, реже звезда. Передача блоками – пакеты (Packet), кадрами (Frame)/

Скорость передачи – 10 Мбит/с.

Принципы работы:

На логическом уровне топология *ШИНА.*

- все устройства (PC) *равноправны.*
- данные, передаваемые одной PC, доступны всем остальным PC.

Форматы кадров технологии Ethernet

Размеры полей блоков (кадров, пакетов) задаются в байтах.

Преамбула - 8	SOF -1	Адрес получателя (DSAP) - 6	Адрес источника (SSAP) - 6	Длина пакета - 2	ДАННЫЕ - 46 ÷1500	Контрольная последовательность - 4

Рис. 2.2. Структура кадра Ethernet

И Ethernet и IEEE 802.3 структуры (рамки) начинаются с чередующегося образца единиц и нолей, называемого преамбулой. Преамбула сообщает станциям получения, что структура (рамка) прибывает.

Байт перед адресом предназначения и в Ethernet и IEEE 802.3 структура (рамка) - " начало структуры (рамки) " (SOF) разделитель. Этот байт заканчивает преамбулу, открывает содержательную часть блока.

Адресы содержатся в аппаратных средствах ЭВМ на Ethernet и IEEE 802.3 карты интерфейса. Первые 3 байта адресов определены IEEE индексируют изготовителя (продавца), в то время как последние 3 байта определяют номер изделия. Исходный адрес - всегда unicast (единственный (отдельный) узел) адрес, в то время как адрес предназначения может быть unicast, групповым или широковещательным («радиопередача» - всем узлам).

В структурах (рамках) Ethernet, область (поле) с 2 байтами после исходного адреса - область (поле) типа. Эта область (поле) определяет протокол с верхним слоем, чтобы получить данные после того, как Ethernet обработка выполнена.

В IEEE 802.3 структуры (рамки), область (поле) с 2 байтами после исходного адреса - область (поле) длины, указывает номер (число) байтов данных, которые следуют в поле ДАННЫЕ (поле данные имеет переменную длину). Эти данные будут в конечном счете посланы протоколу верхнего слоя.

Поле проверки - FCS область с 4 байтами, содержащая циклический «чек» - избыточные контрольные биты (CRC), значения которых вычисляются с учетом значений битов всех полей кадра, кроме битов преамбулы и разделителя. CRC создан устройством посылки и повторно рассчитан устройством получения, чтобы проверить возможное повреждение (ущерб), которое могло бы произойти со структурой (рамкой) в транзите.

Стандарт на технологию Ethernet, описанный в документе 802.3, дает описание единственного формата кадра MAC-уровня. Кадр MAC-уровня должен вкладываться кадр уровня LLC, описанный в документе 802.2.

- Стандарт 802.3 определяет восемь полей заголовка. Дополнительное поле -*поле заполнения* (после поля данных) состоит из такого количества байтов заполнителей, которое обеспечивает определенную минимальную длину поля данных (46 байт). Это обеспечивает корректную работу механизма обнаружения коллизий. Если длина поля данных достаточна, то поле заполнения в кадре не появляется.

В таблице 2 приведены данные о том, какие типы кадров Ethernet обычно поддерживают реализации популярных протоколов сетевого уровня.

Таблица 2

Тип кадра	Сетевые протоколы
Ethernet_II	IPX, IP, AppleTalk Phase I
Ethernet 802.3	IPX

Стандарт Token Ring

Сети стандарта Token Ring используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо - общий разделяемый ресурс, и для доступа к нему используется детерминированный алгоритм, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование кольца передается с помощью кадра специального формата, называемого маркером или токеном.

Стандарт Token Ring был принят комитетом 802.5 в 1985 году. В это же время компания IBM приняла стандарт Token Ring в качестве своей основной сетевой технологии. 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 Мб/с и 16 Мб/с. Первая скорость определена в стандарте 802.5, а вторая является новым стандартом де-факто, появившимся в результате развития технологии Token Ring. Смешение станций, работающих на различных скоростях, в одном кольце не допускается.

Сети Token Ring, работающие со скоростью 16 Мб/с, имеют и некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мб/с.

Право на доступ к среде передается циклически от станции к станции по логическому кольцу. Кольцо образуется отрезками кабеля, соединяющими соседние станции. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения - *маркер (токен)*.

Получив маркер, станция анализирует его, при необходимости модифицирует 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.

При поступлении кадра данных к одной или нескольким станциям, эти станции копируют для себя этот кадр и вставляют в этот кадр подтверждение приема. Станция, выдавшая кадр данных в кольцо, при

обратном его получении с подтверждением приема изымает этот кадр из кольца и выдает новый маркер для обеспечения возможности другим станциям сети передавать данные.

На рисунке 2.18 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.

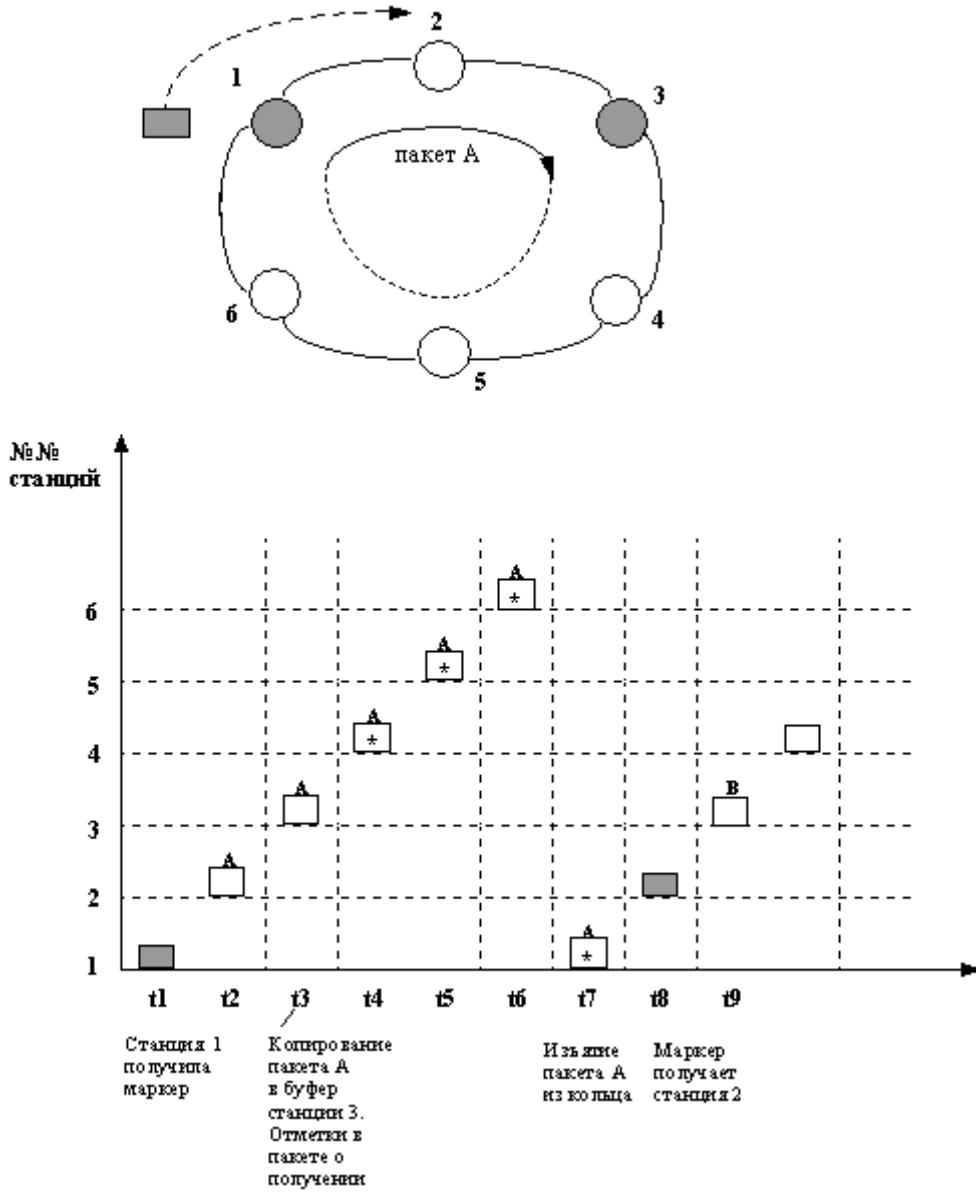


Рис. 2.18. Принцип маркерного доступа

Время удержания одной станцией маркера ограничивается *тайм-аутом удержания маркера,* после истечении которого станция обязана передать маркер далее по кольцу.

В сетях Token Ring 16 Мб/с используется также несколько другой алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release).* В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно и приближается к 80 % от номинальной.

Для различных видов сообщений передаваемым данным могут назначаться различные *приоритеты.*

Каждая станция имеет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции).

Не все станции в кольце равны. Одна из станций обозначается как *активный монитор,* что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление

тайм-аутом в кольце, порождает новые маркеры (если необходимо), чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор отказал по какой-либо причине, существует механизм, с помощью которого другие станции (резервные мониторы) могут договориться, какая из них будет новым активным монитором.

В Token Ring существует три различных формата кадров: маркера, кадра данных, прерывающей последовательности

Маркер. Кадр маркера состоит из трех полей, каждое длиной в один байт.

- *Поле начального ограничителя* появляется в начале маркера, а также в начале любого кадра, проходящего по сети. Поле состоит из уникальной серии электрических импульсов, которые отличаются от тех импульсов, которыми кодируются единицы и нули в байтах данных. Поэтому начальный ограничитель нельзя спутать ни с какой битовой последовательностью.
- *Поле контроля доступа.* Разделяется на четыре элемента данных:
  PPP T M RRR, где PPP - биты приоритета, T - бит маркера, M - бит монитора, RRR - резервные биты.

Бит маркера имеет значение 0 для маркера и 1 для кадра.

- *Поле конечного ограничителя* - последнее поле маркера. Так же, как и поле начального ограничителя, это поле содержит уникальную серию электрических импульсов, которые нельзя спутать с данными.

Кадр данных

Кадр данных состоит из нескольких групп полей:

- последовательность начала кадра;
- адрес получателя;
- адрес отправителя;
- данные;
- последовательность контроля кадра;
- последовательность конца кадра.

Кадр данных может переносить данные либо для управления кольцом (данные MAC-уровня), либо пользовательские данные (LLC-уровня).

Прерывающая последовательность

Состоит из двух байтов, содержащих начальный ограничитель и конечный ограничитель. Прерывающая последовательность может появиться в любом месте потока битов и сигнализирует о том, что текущая передача кадра или маркера отменяется.

В сети Token Ring на уровнях MAC и LLC применяются процедуры без установления связи, но с подтверждением получения кадров.

16. Протокол LLC уровня управления логическим соединением

Протокол LLC уровня управления логическим каналом

В основу протокола LLC положен протокол HDLC (High-level Data Link Control Procedure), широко использующийся в территориальных сетях.

В соответствии со стандартом 802.2 уровень управления логическим каналом LLC предоставляет верхним уровням три типа процедур:

- LLC1 - сервис без установления соединения и без подтверждения;
- LLC2 - сервис с установлением соединения и подтверждением;
- LLC3 - сервис без установления соединения, но с подтверждением.

Этот набор процедур является общим для всех методов доступа к среде, определенных стандартами 802.3-802.5.

Сервис без установления соединения и без подтверждения LLC1 дает пользователю средства для передачи данных с минимумом издержек. Обычно, этот вид сервиса используется тогда, когда такие функции как восстановление данных после ошибок и упорядочивание данных выполняются протоколами вышележащих уровней, поэтому нет нужды дублировать их на уровне LLC.

Сервис с установлением соединений и с подтверждением LLC2 дает пользователю возможность установить логическое соединение перед началом передачи любого блока данных и, если это требуется, выполнить процедуры восстановления после ошибок и упорядочивание потока этих блоков в рамках установленного соединения. Протокол LLC2 во многом аналогичен протоколам семейства HDLC (LAP-B, LAP-D, LAP-M), которые применяются в глобальных сетях для обеспечения надежной передачи кадров на зашумленных линиях.

(LAP-B – работает в территориальных сетях (X.25);

LAP-D – работает в сетях ISDN

LAP-M – в современных модемах)

В некоторых случаях (например, при использовании сетей в системах реального времени, управляющих промышленными объектами), когда временные издержки установления логического соединения перед отправкой данных неприемлемы, а подтверждение корректности приема переданных данных необходимо, базовый сервис без установления соединения и без подтверждения не подходит. Для таких случаев предусмотрен дополнительный сервис, называемый сервисом *без установления соединения, но с подтверждением LLC3*.

Чаще всего в локальных сетях используются протоколы LLC1. Это объясняется тем, что кабельные каналы локальных сетей обеспечивают низкую вероятность искажений бит и потери кадров. Поэтому, использование повышающего надежность обмена протокола LLC2 часто приводит к неоправданной избыточности, только замедляющей общую пропускную способность стека коммуникационных протоколов.

Структура кадров LLC

По своему назначению все кадры уровня LLC (называемые в стандарте 802.2 блоками данных - Protocol Data Unit, PDU) подразделяются на три типа - информационные, управляющие и ненумерованные:

- *Информационные кадры* предназначены для передачи информации в процедурах с установлением логического соединения и должны обязательно содержать поле информации. В процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна.
- *Управляющие кадры* предназначены для передачи команд и ответов в процедурах с установлением логического соединения, в том числе запросов на повторную передачу искаженных информационных блоков.
- *Ненумерованные кадры* предназначены для передачи ненумерованных команд и ответов, выполняющих в процедурах без установления логического соединения передачу информации, идентификацию и тестирование LLC-уровня, а в процедурах с установлением логического соединения - установление и разъединение логического соединения, а также информирование об ошибках.

Все типы кадров уровня LLC имеют единый формат (рис. 2.1). Они содержат четыре поля:

- адрес точки входа сервиса назначения (Destination Service Access Point, DSAP),
- адрес точки входа сервиса источника (Source Service Access Point, SSAP),
- управляющее поле (Control)
- поле данных (Data)

Кадр LLC обрамляется двумя однобайтовыми полями "Флаг", имеющими значение 01111110. Флаги используются на MAC-уровне для определения границ блока. (Отметим, что формат кадров LLC, за исключением поля адреса точки входа сервиса источника, соответствует формату кадра HDLC, а также одного из вариантов протокола HDLC - протокола LAP-B, используемого в сетях X.25).

Флаг (01111110)	Адрес точки входа сервиса назначения DSAP	Адрес точки входа сервиса источника SSAP	Управляющее поле Control	Данные Data	Флаг (01111110)

Рис.2. 1. Структура LLC-кадра стандарта 802-2

Поле данных кадра LLC предназначено для передачи по сети пакетов протоколов верхних уровней - IP, IPX, AppleTalk, DECnet, в редких случаях - прикладных протоколов, когда те не пользуются сетевыми протоколами, а вкладывают свои сообщения непосредственно в кадры канального уровня. Поле данных может отсутствовать в управляющих кадрах и некоторых ненумерованных кадрах.

Поле управления (один байт) используется для обозначения типа кадра данных - информационный, управляющий или ненумерованный. Кроме этого, в этом поле указываются порядковые номера отправленных и успешно принятых кадров, если подуровень LLC работает по процедуре LLC2 с установлением соединения. Формат поля управления полностью совпадает с форматом поля управления кадра LAP-B.

Поля DSAP и SSAP позволяют указать, какой сервис верхнего уровня пересылает данные с помощью этого кадра. Программному обеспечению узлов сети при получении кадров канального уровня

необходимо распознать, какой протокол вложил свой пакет в поле данных поступившего кадра, для того, чтобы передать извлеченный из кадра пакет нужному протоколу для последующей обработки.

18. Структура стандартов IEEE 802

При организации взаимодействия узлов в локальных сетях (ЛС) основная роль отводится протоколу канального уровня.

Для удешевления аппаратных и программных решений совместное использование кабелей (коммуникационной среды) всеми компьютерами сети в режиме *разделения времени*.

Использование в локальных сетях очень простых конфигураций (общая шина и кольцо) – базовые конфигурации. Базовые конфигурации стали элементарными структурами ЛС, которые соединяют друг с другом, образуя основные и резервные пути между узлами.

Базовые технологии ЛС - Ethernet, и Token Ring специфицированы стандартами IEEE – 802.1 – 802.5 (Institute of Electronic and Electrical Enqineers).

Стандарты семейства IEEE 802.x охватывают только два нижних уровня семиуровней 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 нашла также свое отражение в разделении канального уровня на два подуровня:

- подуровень управления доступом к среде (Media Access Control, MAC)

- подуровень логической передачи данных (Logical Link Control, LLC).

Функции уровней

Уровень OSI	Элемент	Методы реализации
Канальный MAC	Логическая топология Доступ к среде ПРД Адресация	Шина, кольцо Состязание, маркер, опрос Физическое устройство (MAC-адрес)
Канальный - LLC	Синхронизация передачи Сервис соединений	Асинхронная, синхронная Управление потоком данных, Контроль ошибок

MAC-уровень 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 следующий подуровень, организующий надежную передачу логических единиц данных - кадров информации.

Уровень LLC отвечает за достоверную передачу кадров данных между узлами, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Для уровня LLC также существует несколько вариантов протоколов, 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 MAC-уровня может применяться с любым типом протокола LLC-уровня и наоборот.

Стандарт IEEE 802 содержит несколько разделов:

- В разделе 802.1 приводятся основные понятия и определения, общие характеристики и требования к локальным сетям.
- Раздел 802.2 определяет подуровень управления логическим каналом LLC.
- Разделы 802.3 - 802.5 регламентируют спецификации различных протоколов подуровня доступа к среде MAC и их связь с уровнем LLC:
  - стандарт 802.3 описывает коллективный доступ с опознаванием несущей и обнаружением конфликтов (Carrier sense multiple access with collision detection - CSMA/CD), прототипом которого является метод доступа стандарта Ethernet;
  - стандарт 802.4 определяет метод доступа к шине с передачей маркера (Token bus network), прототип - ArcNet;
  - стандарт 802.5 описывает метод доступа к кольцу с передачей маркера (Token ring network), прототип - Token Ring.

Для каждого из этих стандартов определены спецификации физического уровня, определяющие среду передачи данных (коаксиальный кабель, витая пара или оптоволоконный кабель), ее параметры, а также методы кодирования информации для передачи по данной среде.

Все методы доступа используют протоколы уровня управления логическим каналом LLC, описанным в стандарте 802.2.

18. Локальная сеть (ЛС) Ethernet

Стандарты технологии Ethernet

Ethernet – это самый распространенный на сегодняшний день стандарт локальных сетей. Общее количество сетей, использующих в настоящее время Ethernet, оценивается в более 5 миллионов.

Ethernet – это сетевой стандарт. Использовались различные варианты случайного доступа к общей радиосреде, получившие название Aloha. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля.

На основе этого стандарта Ethernet был разработан стандарт IEEE 802.3, который во многом совпадает со своим предшественником, но некоторые различия все же имеются. В то время, как в стандарте IEEE 802.3 различаются уровни MAC и LLC, в оригинальном Ethernet оба эти уровня объединены в единый канальный уровень. В Ethernet определяется протокол тестирования конфигурации (Ethernet Configuration Test Protocol), который отсутствует в IEEE 802.3. Несколько отличается и формат кадра, хотя минимальные и максимальные размеры кадров в этих стандартах совпадают.

Для передачи двоичной информации по кабелю для всех вариантов физического уровня технологии Ethernet используется манчестерский код.

Все виды стандартов Ethernet используют один и тот же метод разделения среды передачи данных - метод CSMA/CD (carrier sense multiply access/collision detection – контроль несущей множественный доступ/обнаружение столкновений).

Топология – шина, реже звезда. Передача блоками – пакеты (Packet), кадрами (Frame)/

Скорость передачи – 10 Мбит/с.

Принципы работы:

На логическом уровне топология *ШИНА.*

- все устройства (PC) *равноправны.*
- данные, передаваемые одной PC, доступны всем остальным PC.

Форматы кадров технологии Ethernet
Размеры полей блоков (кадров, пакетов) задаются в байтах.

Преамбула - 8	S O F -1	Адрес получателя (DSAP) - 6	Адрес источника (SSAP) - 6	Длина пакета - 2	ДАННЫЕ - 46 ÷1500	Контрольная последовательность - 4

Рис. 2.2. Структура кадра Ethernet

И Ethernet и IEEE 802.3 структуры (рамки) начинаются с чередующегося образца единиц и нолей, называемого преамбулой. Преамбула сообщает станциям получения, что структура (рамка) прибывает.

Байт перед адресом предназначения и в Ethernet и IEEE 802.3 структура (рамка) - " начало структуры (рамки) " (SOF) разделитель. Этот байт заканчивает преамбулу, открывает содержательную часть блока.

Адресы содержатся в аппаратных средствах ЭВМ на Ethernet и IEEE 802.3 карты интерфейса. Первые 3 байта адресов определены IEEE индексируют изготовителя (продавца), в то время как последние 3 байта определяют номер изделия. Исходный адрес - всегда unicast (единственный (отдельный) узел) адрес, в то время как адрес предназначения может быть unicast, групповым или широковещательным («радиопередача» - всем узлам).

В структурах (рамках) Ethernet, область (поле) с 2 байтами после исходного адреса - область (поле) типа. Эта область (поле) определяет протокол с верхним слоем, чтобы получить данные после того, как Ethernet обработка выполнена.

В IEEE 802.3 структуры (рамки), область (поле) с 2 байтами после исходного адреса - область (поле) длины, указывает номер (число) байтов данных, которые следуют в поле ДАННЫЕ (поле данные имеет переменную длину). Эти данные будут в конечном счете посланы протоколу верхнего слоя.

Поле проверки - FCS область с 4 байтами, содержащая циклический «чек» - избыточные контрольные биты (CRC), значения которых вычисляются с учетом значений битов всех полей кадра, кроме битов преамбулы и разделителя. CRC создан устройством посылки и повторно рассчитан устройством получения, чтобы проверить возможное повреждение (ущерб), которое могло бы произойти со структурой (рамкой) в транзите.

Стандарт на технологию Ethernet, описанный в документе 802.3, дает описание единственного формата кадра MAC-уровня. Кадр MAC-уровня должен вкладываться кадр уровня LLC, описанный в документе 802.2.

- Стандарт 802.3 определяет восемь полей заголовка. Дополнительное поле -*поле заполнения* (после поля данных) состоит из такого количества байтов заполнителей, которое обеспечивает определенную минимальную длину поля данных (46 байт). Это обеспечивает корректную работу механизма обнаружения коллизий. Если длина поля данных достаточна, то поле заполнения в кадре не появляется.

В таблице 2 приведены данные о том, какие типы кадров Ethernet обычно поддерживают реализации популярных протоколов сетевого уровня.

Таблица 2

Тип кадра	Сетевые протоколы
Ethernet_II	IPX, IP, AppleTalk Phase I
Ethernet 802.3	IPX

19. Параметры Ethernet

Основные параметры операций передачи и приема кадров Ethernet, подобраны так, чтобы при нормальной работе узлов *коллизии* всегда четко распознавались.

Станция, которая хочет передать кадр, должна сначала с помощью MAC-узла упаковать данные в кадр соответствующего формата. Затем для предотвращения смешения сигналов с сигналами другой передающей станции, MAC-узел должен прослушивать электрические сигналы на кабеле и в случае обнаружения несущей частоты 10 МГц отложить передачу своего кадра. После окончания передачи по кабелю станция должна выждать небольшую дополнительную паузу, называемую *межкадровым интервалом (interframe gap)*, что позволяет узлу назначения принять и обработать передаваемый кадр, и после этого начать передачу своего кадра.

Одновременно с передачей битов кадра приемно-передающее устройство узла следит за принимаемыми по общему кабелю битами, чтобы вовремя обнаружить коллизию. Если коллизия не обнаружена, то передается весь кадр, поле чего MAC-уровень узла готов принять кадр из сети либо от LLC-уровня.

Если же фиксируется коллизия, то MAC-узел прекращает передачу кадра и посылает jam-последовательность, усиливающую состояние коллизии. После посылки в сеть jam-последовательности MAC-узел делает случайную паузу и повторно пытается передать свой кадр.

В случае повторных коллизий существует максимально возможное *число попыток повторной передачи кадра (attempt limit)*, которое равно 16. При достижении этого предела фиксируется ошибка передачи кадра, сообщение о которой передается протоколу верхнего уровня.

Для того, чтобы уменьшить интенсивность коллизий, каждый MAC-узел с каждой новой попыткой случайным образом увеличивает длительность паузы между попытками. Временное расписание длительности паузы определяется на основе *усеченного двоичного экспоненциального алгоритма отсрочки (truncated binary exponential backoff)*. Пауза всегда составляет целое число так называемых интервалов отсрочки.

Интервал отсрочки (slot time) - это время, в течение которого станция гарантированно может узнать, что в сети нет коллизии. Это время тесно связано с другим важным временным параметром сети - *окном коллизий (collision window)*. Окно коллизий равно времени двукратного прохождения сигнала между

самыми удаленными узлами сети - наихудшему случаю задержки, при которой станция еще может обнаружить, что произошла коллизия. Интервал отсрочки выбирается равным величине окна коллизий плюс некоторая дополнительная величина задержки для гарантии:

интервал отсрочки = окно коллизий + дополнительная задержка

В стандартах 802.3 большинство временных интервалов измеряется в количестве межбитовых интервалов, величина которых для битовой скорости 10 Мб/с составляет 0.1 мкс и равна времени передачи одного бита.

Величина интервала отсрочки в стандарте 802.3 определена равной 512 битовым интервалам, и эта величина рассчитана для максимальной длины коаксиального кабеля в 2.5 км. Величина 512 определяет и минимальную длину кадра в 64 байта, так как при кадрах меньшей длины станция может передать кадр и не успеть заметить факт возникновения коллизии из-за того, что искаженные коллизией сигналы дойдут до станции в наихудшем случае после завершения передачи. Такой кадр будет просто потерян.

Время паузы после N-ой коллизии полагается равным L интервалам отсрочки, где L - случайное целое число, равномерно распределенное в диапазоне [0, 2N]. Величина диапазона растет только до 10 попытки (напомним, что их не может быть больше 16), а далее диапазон остается равным [0, 210], то есть [0, 1024]. Значения основных параметров процедуры передачи кадра стандарта 802.3 приведено в таблице 1.

Таблица 1.

Битовая скорость	10 Мб/с
Интервал отсрочки	512 битовых интервалов
Межкадровый интервал	9.6 мкс
Максимальное число попыток передачи	16
Максимальное число возрастания диапазона паузы	10
Длина jam-последовательности	32 бита
Максимальная длина кадра (без преамбулы)	1518 байтов
Минимальная длина кадра (без преамбулы)	64 байта (512 бит)
Длина преамбулы	64 бита

Учитывая приведенные параметры, нетрудно рассчитать максимальную производительность сегмента Ethernet в таких единицах, как число переданных пакетов минимальной длины в секунду (packets-per-second, pps). Количество обрабатываемых пакетов Ethernet в секунду часто используется при указании внутренней производительности мостов и маршрутизаторов, вносящих дополнительные задержки при обмене между узлами. Поэтому интересно знать чистую максимальную производительность сегмента Ethernet в идеальном случае, когда на кабеле нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами.

Так как размер пакета минимальной длины вместе с преамбулой составляет 64+8 = 72 байта или 576 битов, то на его передачу затрачивается 57.6 мкс. Прибавив межкадровый интервал в 9.6 мкс, получаем,

что период следования минимальных пакетов равен 67.2 мкс. Это соответствует максимально возможной пропускной способности сегмента Ethernet в 14880 п/с.

20. Методика расчета конфигурации Ethernet

Сеть Ethernet состоит из сегментов различной физической природы.

Три основных условия корректной работы:

- Количество станций в сети не превышает 1024 (с учетом ограничений для коаксиальных сегментов).
- Удвоенная задержка распространения сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети не превышает 575 битовых интервалов.
- Сокращение межкадрового расстояния (Interpacket Gap Shrinkage) при прохождении последовательности кадров через все повторители не более, чем на 49 битовых интервалов (напомним, что при отправке кадров станция обеспечивает начальное межкадровое расстояние в 96 битовых интервалов).

Правила конфигурирования определяют максимальное количество повторителей и максимальную длину сегментов каждого типа.

При прохождении кадра через повторитель межкадровое расстояние уменьшается. Каждый пакет, принимаемый повторителем, ресинхронизируется для исключения дрожания сигналов, накопленного при прохождении последовательности импульсов по кабелю и через интерфейсные схемы. Процесс ресинхронизации обычно увеличивает длину преамбулы, что уменьшает межкадровый интервал. При прохождении кадров через несколько повторителей межкадровый интервал может уменьшиться настолько, что сетевым адаптерам в последнем сегменте не хватит времени на обработку предыдущего кадра, в результате чего кадр будет просто потерян. Поэтому не допускается суммарное уменьшение межкадрового интервала более чем на 49 битовых интервалов. Величину уменьшения межкадрового расстояния при переходе между соседними сегментами обычно называют в англоязычной литературе Segment Variability Value, SVV, а суммарную величину уменьшения межкадрового интервала при прохождении всех повторителей - Path Variability Value, PVV. Очевидно, что величина PVV равна сумме SVV всех сегментов, кроме последнего.

Расчет PDV

Для расчетов используются справочные данные, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и в различных физических средах. В таблице 3 приведены данные, необходимые для расчета значения PDV для всех физических стандартов сетей Ethernet, взятые из справочника Technical Reference Pocket Guide (Volume 4, Number 4) компании Bay Networks.

Таблица 3.

Тип сегмента	База левого сегмента	База промежуточного сегмента	База правого сегмента	Задержка среды на 1 м	Максимальная длина сегмента

10 Base-5	11.8	46.5	169.5	0.0866	500
10 Base-2	11.8	46.5	169.5	0.1026	185
10 Base-T	15.3	42.0	165.0	0.113	100
10 Base-FB	-	24.0	-	0.1	2000
10 Base-FL	12.3	33.5	156.5	0.1	2000
FO IRL	7.8	29.0	152.0	0.1	1000
AUI (> 2 м)	0	0	0	0.1026	2+48

Поясним терминологию, использованную в этой таблице, на примере сети, изображенной на рисунке 2.4.

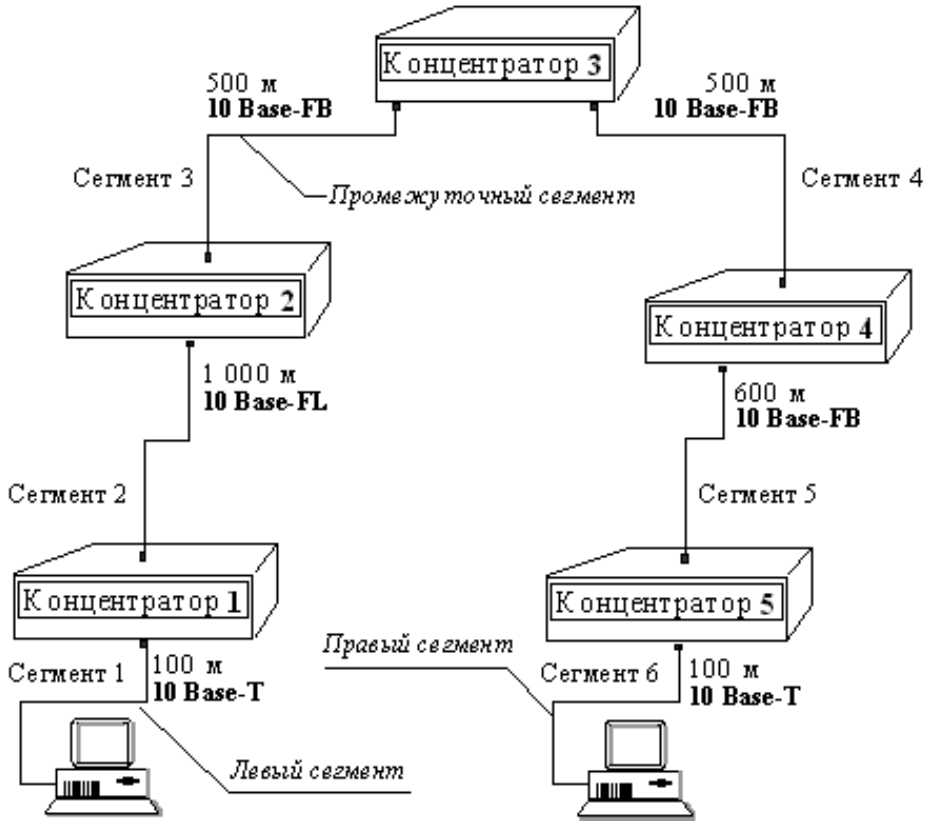


Рис. 2.4. Пример сети Ethernet, состоящей из сегментов различных физических стандартов

Левым сегментом называется сегмент, в котором начинается путь сигнала от выхода передатчика (выход Tx) конечного узла. Затем сигнал проходит через *промежуточные* сегменты и доходит до приемника (вход Rx) наиболее удаленного узла наиболее удаленного сегмента, который называется

правым. С каждым сегментом связана постоянная задержка, названная *базой*, которая зависит только от типа сегмента и от положения сегмента на пути сигнала (левый, промежуточный или правый). Кроме этого, с каждым сегментом связана *задержка распространения сигнала* вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени распространения сигнала по одному метру кабеля (в битовых интервалах) на длину кабеля в метрах.

Общее значение PDV равно сумме базовых и переменных задержек всех сегментов сети. Значения констант в таблице даны с учетом удвоения величины задержки при круговом обходе сети сигналом, поэтому удваивать полученную сумму не нужно.

Так как левый и правый сегмент имеют различные величины базовой задержки, то в случае различных типов сегментов на удаленных краях сети необходимо выполнить расчеты дважды: один раз принять в качестве левого сегмента сегмент одного типа, а во второй раз - сегмент другого типа, а результатом считать максимальное значение PDV. В нашем примере крайние сегменты сети принадлежат к одному типу - стандарту 10Base-T, поэтому двойной расчет не требуется, но если бы они были сегментами разного типа, то в первом случае нужно было бы принять в качестве левого сегмент между станцией и концентратором 1, а во втором считать левым сегмент между станцией и концентратором 5.

Рассчитаем значение PDV для нашего примера.

Левый сегмент 1: 15.3 (база) + 100 м ґ 0.113 /м = 26.6

Промежуточный сегмент 2: 33.5 + 1000 ґ 0.1 = 133.5

Промежуточный сегмент 3: 24 + 500 ґ 0.1 = 74.0

Промежуточный сегмент 4: 24 + 500 ґ 0.1 = 74.0

Промежуточный сегмент 5: 24 + 600 ґ 0.1 = 84.0

Правый сегмент 6: 165 + 100 ґ 0.113 = 176.3

Сумма всех составляющих дает значение PDV, равное 568.4.

Так как значение PDV меньше максимально допустимой величины 575, то эта сеть проходит по величине максимально возможной задержки оборота сигнала. Несмотря на то, что ее общая длина больше 2500 метров.

Расчет PVV

Для расчета PVV также можно воспользоваться табличными значениями максимальных величин уменьшения межкадрового интервала при прохождении повторителей различных физических сред (таблица 4 взята из того же справочника, что и предыдущая).

Таблица 4.

Тип сегмента	Передающий сегмент	Промежуточный сегмент
10Base-5 или 10Base-2	16	11

10Base-FB	-	2
10Base-FL	10.5	8
10Base-T	10.5	8

В соответствии с этими данными рассчитаем значение PVV для нашего примера.

Левый сегмент 1 10Base-T: дает сокращение в 10.5 битовых интервалов

Промежуточный сегмент 2 10Base-FL: 8

Промежуточный сегмент 3 10Base-FB: 2

Промежуточный сегмент 4 10Base-FB: 2

Промежуточный сегмент 5 10Base-FB: 2

Сумма этих величин дает значение PVV, равное 24.5, что меньше предельного значения в 49 битовых интервалов.

В результате, приведенная в примере сеть по всем параметрам соответствует стандартам Ethernet.

21. Fast Ethernet

Fast Ethernet является развитием классического Ethernet'a. В мае 1995 года комитет IEEE принял спецификацию Fast Ethernet в качестве стандарта 802.3u, которая представляет собой дополнение к существующему стандарту 802.3. Отличия Fast Ethernet от Ethernet сосредоточены на физическом уровне.

Более сложная структура физического уровня технологии Fast Ethernet вызвана тем, что в ней используется три варианта кабельных систем - оптоволокно, 2-х парная витая пара категории 5 и 4-х парная витая пара категории 3.

Основными достоинствами технологии Fast Ethernet являются:

- увеличение пропускной способности сегментов сети до 100 Мб/с;
- сохранение метода случайного доступа Ethernet;
- сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных - витой пары и оптоволоконного кабеля.

Указанные свойства позволяют осуществлять постепенный переход от сетей 10Base-T - наиболее популярного на сегодняшний день варианта Ethernet - к скоростным сетям, сохраняющим значительную преемственность с хорошо знакомой технологией: Fast Ethernet не требует коренного переобучения персонала и замены оборудования во всех узлах сети.

Официальный стандарт 100Base-T (802.3u) установил три различных спецификации для физического уровня (в терминах семиуровневой модели OSI) для поддержки следующих типов кабельных систем:

- 100Base-TX для двухпарного кабеля на неэкранированной витой паре UTP категории 5, или экранированной витой паре STP Type 1;
- 100Base-T4 для четырехпарного кабеля на неэкранированной витой паре UTP категории 3, 4 или 5;

- 100Base-FX для многомодового оптоволоконного кабеля.

Метод доступа к среде CSMA/CD. Подуровни LLC и MAC в стандарте Fast Ethernet не претерпели изменений.

Подуровень LLC обеспечивает интерфейс протокола Ethernet с протоколами вышележащих уровней, например, с IP или IPX.

Подуровень MAC ответственен за формирование кадра Ethernet, получение доступа к разделяемой среде передачи данных и за отправку с помощью физического уровня кадра по физической среде узлу назначения.

MAC-подуровень каждого узла сети получает от физического уровня информацию о состоянии разделяемой среды.

MAC-подуровень узла приемника, который получает биты кадра от своего физического уровня, проверяет поле адреса кадра, и если адрес совпадает с его собственным, то он копирует кадр в свой буфер. Затем он проверяет, не содержит ли кадр специфические ошибки: по контрольной сумме (FCS error), по максимально допустимому размеру кадра (jabber error), по минимально допустимому размеру кадра (runts), по неверно найденным границам байт (alignment error). Если кадр корректен, то его поле данных передается на LLC-подуровень, если нет - то отбрасывается.

Форматы кадров технологии Fast Ethernet не отличаются от форматов кадров технологий 10-Мегабитного Ethernet'a. На рисунке 2.10 приведен формат MAC-кадра Ethernet, а также временные параметры его передачи по сети для скорости 10 Мб/с и для скорости 100 Мб/с.

Все времена передачи кадров Fast Ethernet в 10 раз меньше соответствующих времен технологии 10-Мегабитного Ethernet'a: межбитовый интервал составляет 10 нс вместо 100 нс, а межкадровый интервал - 0.96 мкс вместо 9.6 мкс соответственно.

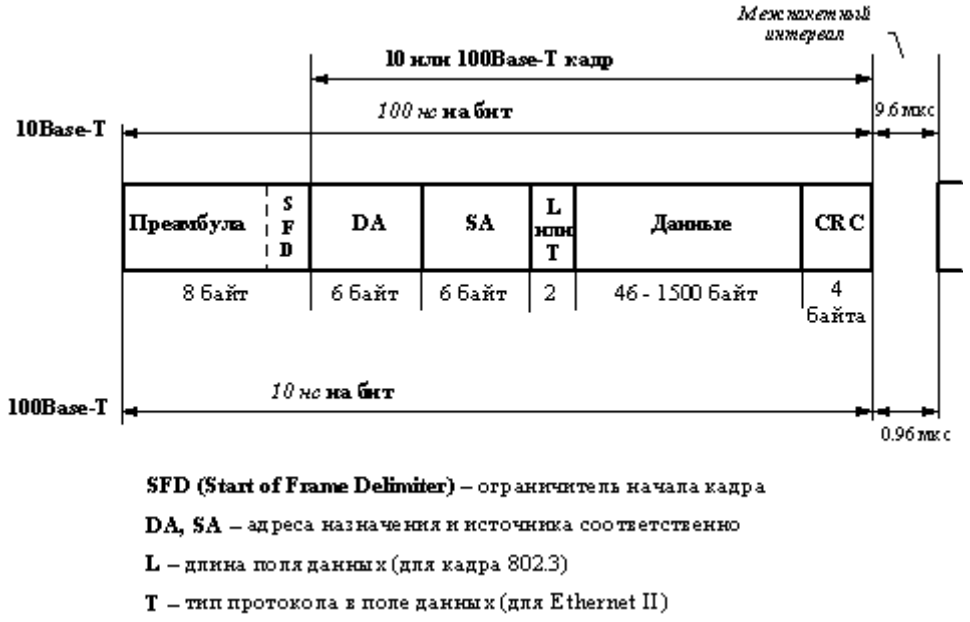


Рис.210. Формат MAC-кадра и времена его передачи

Спецификации физического уровня Fast Ethernet

Для технологии Fast Ethernet разработаны различные варианты физического уровня, отличающиеся типом кабеля, электрическими параметрами импульсов, способом кодирования сигналов и количеством

используемых в кабеле проводников. Поэтому физический уровень Fast Ethernet имеет более сложную структуру, чем классический Ethernet. Физический уровень состоит из трех подуровней:

- Уровень согласования (reconciliation sublayer).
- Независимый от среды интерфейс (Media Independent Interface, MII).
- Устройство физического уровня (Physical layer device, PHY).

Физический уровень PHY ответственен за прием данных в параллельной форме от MAC-подуровня, трансляцию их в один (TX или FX) или три последовательных потока бит (T4) с возможностью побитной синхронизации и передачу их через разъем на кабель. Аналогично, на приемном узле уровень PHY должен принимать сигналы по кабелю, определять моменты синхронизации бит, извлекать биты из физических сигналов, преобразовывать их в параллельную форму и передавать подуровню MAC.

Интерфейс MII поддерживает независимый от используемой физической среды способ обмена данными между MAC-подуровнем и подуровнем PHY. MII располагается между MAC-подуровнем и подуровнями кодирования сигнала, которых в стандарте Fast Ethernet три - FX, TX и T4.

Подуровень согласования нужен для того, чтобы согласовать работу подуровня MAC с интерфейсом MII.

22. Gigabit Ethernet

Стандарт Gigabit Ethernet IEEE 802.3z был принят в конце 1998 года.
Применяется та же самая стратегия, что и в сети Fast Ethernet:

- сохранен протокол CSMA/CD;

- формат кадра, что и для 10-Мбит/с и 100-Мбит/с предшественников.

Изменен носитель. Спецификация стандарта IEEE 802.3z включает альтернативные варианты:

-1000 BASE-LX. Длинноволновый выриант. Источник – лазер. Оптоволоконный многомодовый кабель Ǿ62,5 µкм или 50 µкм, поддерживающий дуплексные линии длиной до 550 м,

или одномодовый кабель Ǿ10 µкм дл. до 5 км. Диапазон волн 1270÷1355 нм

- 1000 BASE-SX Коротковолновый вариант. Оптоволоконный одномодовый кабель Ǿ62,5 µкм и длиной до 275 м или Ǿ50 µкм, длиной до 550 м, дуплексные линии. Диапазон волн от 770÷860 нм

- 1000 BASE-CX. Устройства в одном помещении или в одной аппаратной стойке. Используются специализированные кабели из витых пар протяженностью не более 25 м (медные перемычки). Каждая линия состоит из отдельной экранированной витой пары, данные по которой передаются в обе стороны.

- 1000 BASE-T. Используется 4 неэкранированные витые пары категории 5 для связи с устройствами до 100 м. Вариант для «бедных».

В связи с ограничениями, накладываемыми методом CSMA/CD на длину кабеля, версия Gigabit Ethernet для разделяемой среды допускает длину связей до 25 метров на витой паре. 25 м – неприемлемо малая длина. Увеличить допустимую длину сегмента можно за счет «расширения носителя» до 512 байт (по отношению к минимальной длине кадра в 64 байта в Ethernet). Увеличение максимальной длины сегмента до 200 м.

Более популярны полнодуплексные версии гигабитного Ethernet'a, работающие только с коммутаторами и допускающие расстояние между узлом и коммутатором в 500 метров для многомодового кабеля и до 2 км для одномодового кабеля.

Кодирование сигналов в Gigabit Ethernet

Кодирование сигналов 8B/10B. Правила выбора кодовых слов:
- ни одно кодовое словоьне должно иметь более 4-х одинаковых битов подряд;
- ни в одном кодовом слове не должно быть более 6-и нулей или 6-и единиц.

Почему так?

a) достаточное количество изменений в потоке данных обеспечивает сиххронизацию приемника с передатчиком;
b) сбалансированному количеству нулей и единиц удается держать постоянную составляющую сигнала на как можно более низком уровне – тогда сигнал проходит через преобразователи без нежелптельных изменений .

Предусмотрен контроль потока – посылка специального служебного кадра, сообщающего о том, что передающей стороне необходимо приостановиться.

33. 10 – гигабиттовая Ethernet

Появление такой сети вызвано непрекращающимся ростом трафика, что связанос:

- увеличением количества соединений;
- увеличением скорости соединений с каждой конечной станцией;
- увеличением быстродействия рабочих станций;
- ростом популярности широкополосных приложений (видео высокого качества);
- рост популярности web-приложений и увеличение web-трафика.

В начале 10 – гигабитовую сеть Ethernet использовали для ЛС.

По мере увеличения спроса на широкополосную связь технология 10 – гигабитовой Ethernet распространяется на серверные «фермы», магистрали и ЛС, охватывающие комплексы зданий.

Эта технология позволяет создавать региональные и глобальные сети, соединяющие удаленные ЛС.

Конкурирует с ATM (Asynchronous Transfer Mode – асинхронный режим доставки). Там, где транспортировка данных реализуется с использованием стека TCP/IP оказывается лучше 10 – гигабитовая Ethernet (не нужно фрагментации кадров – ATM имеет фиксированную длину кадра в 53 байта).

23. Fibre Cannel

Fibre Channel совмещает в себе два аспекта обмена данными с процессором: канал ввода-вывода и сетевую связь.

Канал ввода-вывода (прямая двухточечная линия связи, аппаратно реализованная) обеспечивает высокую скорость ПД на короткие расстояния. Передаются только данные пользователя независимо от формата или назначения данных. Логика этой связи обеспечивает минимальные затраты на управление и защиту передаваемых данных.

Сеть представляет собой набор связанных точек доступа с программной структурой протоколов, обеспечивающей обмен данными.

Интерфейс Fibre Channel разработан для объединения лучших качеств обеих технологий – простоты и скорости каналов ввода-вывода и гибкости и взаимосвязанности сетевых технологий.

Элементами сети Fibre Channel являются конечные узлы (nodes) и набор коммутирующих элементов, называемый каркасом (fabric) (рис. 2.17)

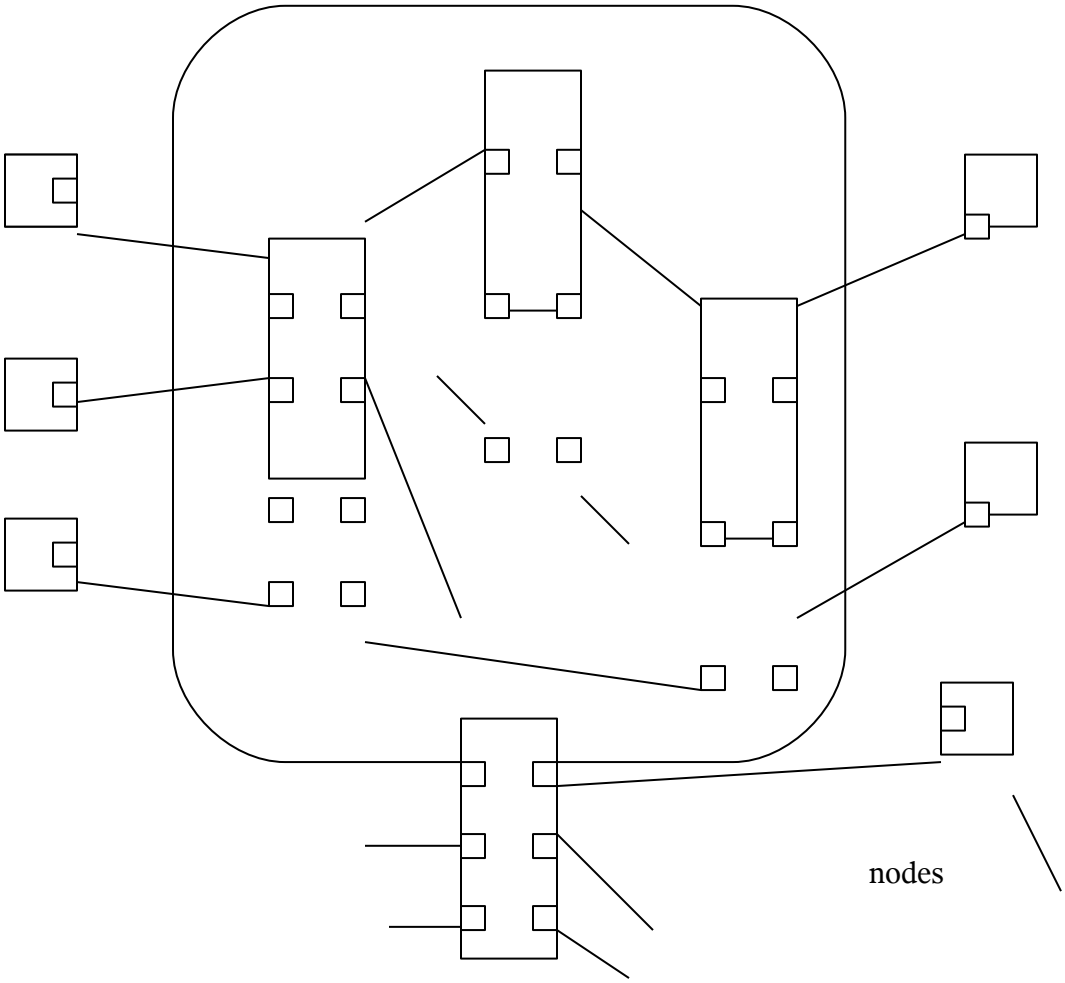


Рис.2.17. Структура сети Fibre Channel

Элементы соединены двухточечными линиями между портами индивидуальных узлов и коммутаторов. Взаимодействие состоит из передачи кадров по двунаправленным двухточечным линиям между портами.

У оконечных узлов – N-порты, у элементов каркаса – F-порты.

Вся маршрутизация кадров между узлами осуществляется каркасом. Каркас может буферировать кадры, что позволяет узлам общаться на разных скоростях ПД.

Поскольку сеть Fibre Channel основана на коммутирующей сети, то не возникает вопроса доступа к несущей. Сеть легко масштабируется.

Архитектура протоколов Fibre Channel

Стандарт FCh описывает 5 уровней.

FC-0. Физический носитель:

- оптоволоконный кабель – ПД на большие расстояния;
- коаксиальный кабель – для выкоких скоростей ПД на короткие расстояния;
- экранированная витая пара для низких скоростей ПД на короткие расстояния.

Скорости от 100 Мбит/с до 3,2 Мбит/с. Расстояния от 33 м до 10 км.

Топология каркаса - произвольная: звезда – один F-элемент (коммутатор, коммутируемая сеть – ячеистая топология.

Индивидуальный N-узел Fibre Channel (оконечная система) ответственен только за управление простым двухточечным соединением между собой и каркасом.

Каркас отвечает за маршрутизацию и обнаружение ошибок.

Помимо каркаса определены еще две топологии:

- двухточечная: два N-порта соединены напрямую без промежуточных коммутаторов каркаса;
- кольцо с арбитражной логикой (до 126 узлов).

Топологии, носители данных и скорости ПД могут комбинироваться.

FC-1 Протокол ПД. Определяет схему кодирования сигнала. Используется NRZI (Non Return to Zero with ones Inverted – потенциальный код с инвесией при единице).

FC-2. Кадровый протокол. Имеет дело с определением форматов кадров, группированием кадров в логические объекты, называемые последовательностями и обменами.

FC-3. Общие службы. Сюда относят групповую рассылку.

FC-4. Отображение. Определяет отображение различных канальных и сетевых протоколов на протоколы Fibre Channel, включая IEEE 802? ATM? IP.

Технология Fibre Channel получила широкое распространение как более совершенное средство соединения периферийных устройств (замена SCSI Small Computer Systems Interface – интерфейс малых компьютерных систем). Конкурирует с Ethernet и ATM.

24. Л С Tokin Ring

Сети стандарта Token Ring используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо - общий разделяемый ресурс, и для доступа к нему используется детерминированный алгоритм, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование кольца передается с помощью кадра специального формата, называемого маркером или токеном.

Стандарт Token Ring был принят комитетом 802.5 в 1985 году. В это же время компания IBM приняла стандарт Token Ring в качестве своей основной сетевой технологии. 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 Мб/с и 16 Мб/с. Первая скорость определена в стандарте 802.5, а вторая является новым стандартом де-факто, появившимся в результате развития технологии Token Ring. Смешение станций, работающих на различных скоростях, в одном кольце не допускается.

Сети Token Ring, работающие со скоростью 16 Мб/с, имеют и некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мб/с.

Право на доступ к среде передается циклически от станции к станции по логическому кольцу. Кольцо образуется отрезками кабеля, соединяющими соседние станции. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения - *маркер (токен)*.

Получив маркер, станция анализирует его, при необходимости модифицирует 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.

При поступлении кадра данных к одной или нескольким станциям, эти станции копируют для себя этот кадр и вставляют в этот кадр подтверждение приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и выдает новый маркер для обеспечения возможности другим станциям сети передавать данные.

На рисунке 2.18 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.

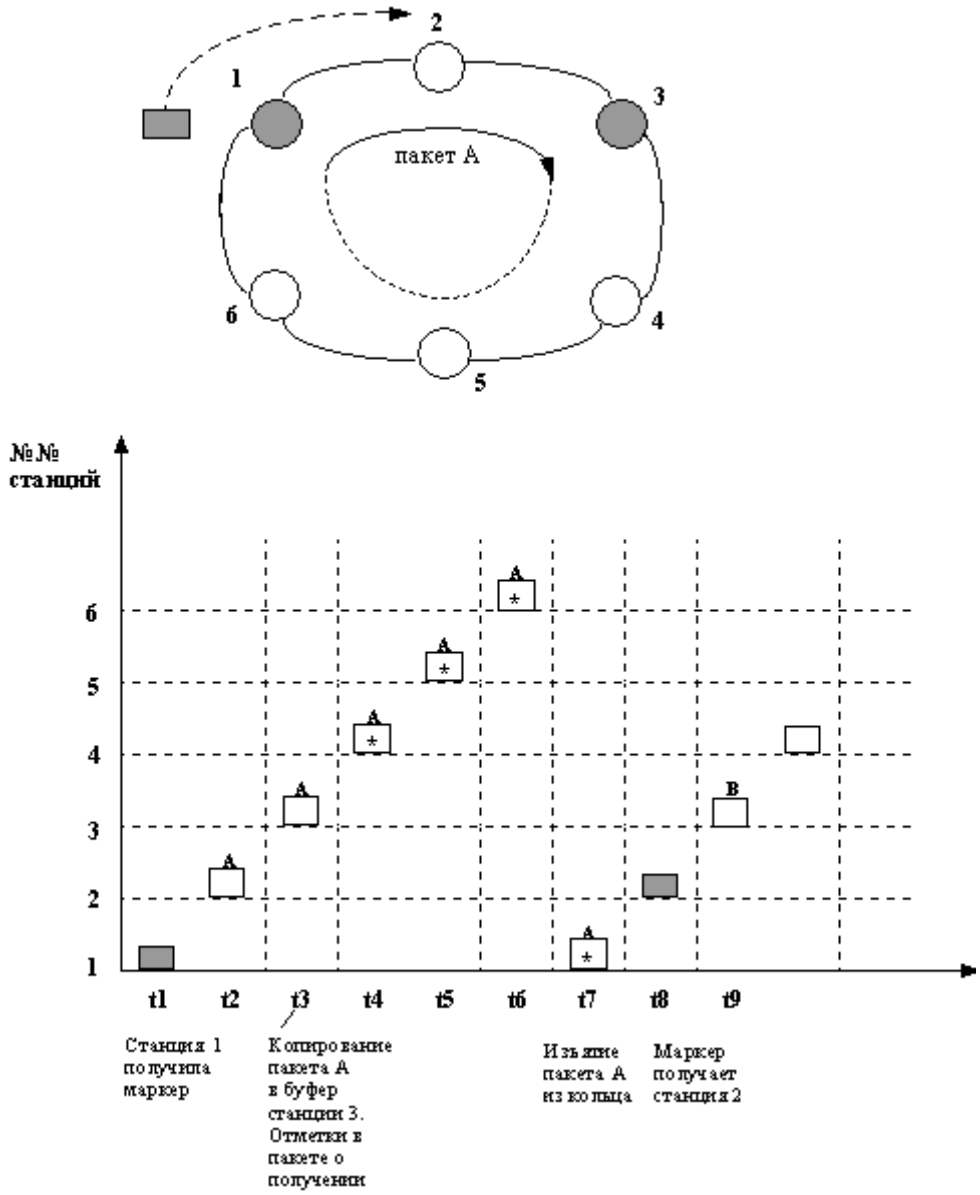


Рис. 2.18. Принцип маркерного доступа

Время удержания одной станцией маркера ограничивается *тайм-аутом удержания маркера,* после истечении которого станция обязана передать маркер далее по кольцу.

В сетях Token Ring 16 Мб/с используется также несколько другой алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release).* В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно и приближается к 80 % от номинальной.

Для различных видов сообщений передаваемым данным могут назначаться различные *приоритеты.*

Каждая станция имеет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции).

Не все станции в кольце равны. Одна из станций обозначается как *активный монитор,* что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление тайм-аутом в кольце, порождает новые маркеры (если необходимо), чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор

отказал по какой-либо причине, существует механизм, с помощью которого другие станции (резервные мониторы) могут договориться, какая из них будет новым активным монитором.

В Token Ring существует три различных формата кадров: маркера, кадра данных, прерывающей последовательности

Маркер. Кадр маркера состоит из трех полей, каждое длиной в один байт.

- *Поле начального ограничителя* появляется в начале маркера, а также в начале любого кадра, проходящего по сети. Поле состоит из уникальной серии электрических импульсов, которые отличаются от тех импульсов, которыми кодируются единицы и нули в байтах данных. Поэтому начальный ограничитель нельзя спутать ни с какой битовой последовательностью.
- *Поле контроля доступа.* Разделяется на четыре элемента данных:
  PPP T M RRR, где PPP - биты приоритета, T - бит маркера, M - бит монитора, RRR - резервные биты.

Бит маркера имеет значение 0 для маркера и 1 для кадра.

- *Поле конечного ограничителя* - последнее поле маркера. Так же, как и поле начального ограничителя, это поле содержит уникальную серию электрических импульсов, которые нельзя спутать с данными.

Кадр данных

Кадр данных состоит из нескольких групп полей:

- последовательность начала кадра;
- адрес получателя;
- адрес отправителя;
- данные;
- последовательность контроля кадра;
- последовательность конца кадра.

Кадр данных может переносить данные либо для управления кольцом (данные MAC-уровня), либо пользовательские данные (LLC-уровня).

Прерывающая последовательность

Состоит из двух байтов, содержащих начальный ограничитель и конечный ограничитель. Прерывающая последовательность может появиться в любом месте потока битов и сигнализирует о том, что текущая передача кадра или маркера отменяется.

В сети Token Ring на уровнях MAC и LLC применяются процедуры без установления связи, но с подтверждением получения кадров.

25. FDDI

Технология *Fiber Distributed Data Interface* - первая технология локальных сетей, которая использовала в качестве среды передачи данных оптоволоконный кабель.

Начальные версии различных составляющих частей стандарта FDDI были разработаны комитетом X3T9.5 в 1986 - 1988 годах, и тогда же появилось первое оборудование - сетевые адаптеры, концентраторы, мосты и маршрутизаторы, поддерживающие этот стандарт.

В настоящее время большинство сетевых технологий поддерживают оптоволоконные кабели в качестве одного из вариантов физического уровня, но FDDI остается наиболее отработанной высокоскоростной технологией, стандарты на которую прошли проверку временем и устоялись, так что оборудование различных производителей показывает хорошую степень совместимости.

Технология FDDI во многом основывается на технологии Token Ring, 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. Узлы 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 (рис. 2.19), 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. 2.19. 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 Token Ring и также называется методом маркерного (или токенного) кольца - token ring (рис. 2.20, а).

Станция может начать передачу своих собственных кадров данных только в том случае, если она получила от предыдущей станции специальный кадр - токен доступа (рис. 2.20, б). После этого она может передавать свои кадры, если они у нее имеются, в течение времени, называемого временем удержания токена - Token Holding Time (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 (upstream neighbor) и последующий сосед (downstream neighbor), определяемые ее физическими связями и направлением передачи информации.

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 (рис. 2.20, 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 FDDI уровня (например, IP), а затем передает исходный кадр по сети последующей станции (рис. 2.20, 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 (рис. 2.20, 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.

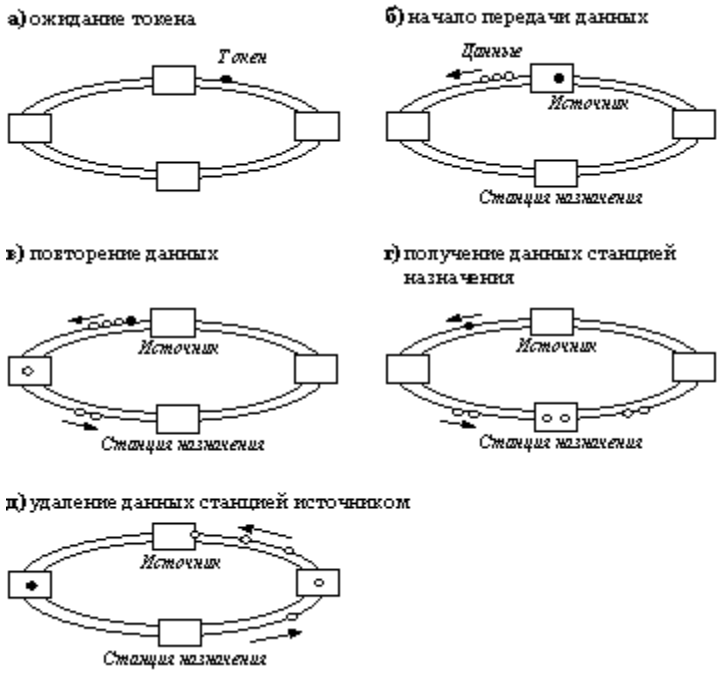


Рис. 2.20. Обработка кадров станциями кольца FDDI

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

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

узлов			витой пары, 72 для неэкранированной витой пары
Тактирование и восстановление после отказов	Распределенная реализация тактирования и восстановления после отказов	Не определены	Активный монитор

26. Коммуникационная система ЛС

В качестве среды обмена сигналами между компьютерами используются кабели и радиоканалы.

Кабели:

коаксиальный (180 м; 500 м; 10 Мбит/с);

витая пара неэкранированная, экранированная (до 100 м, до 100 Мбит/с);

оптоволоконный (до нескольких Гбит/с; до десятков *км* без усиления).

Радио: диапазоны КВ, УКВ.СВЧ.

Простои до 70% происходят из-за низкого качества кабельных систем.

Рекомендуется использовать ***структурированную кабельную систему*** (Structured Cabling System,SCS) (см. рис. 2.5).

SCS – это набор коммутационных элементов(кабелей, разъемов, коннекторов (трансиверов), кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в сетях ЭВМ.

Преимущества SCS:

- универсальность. Может быть единая среда для передачи различных сообщений (речь, данные, видео, сигналы датчиков пожарной опасности, охранной системы;
- расширяемость (масштабируемость) сети: SCS является модульной системой – легко наращивать, переходить на более совершенное оборудование;
- эффективность обслуживания: облегчает обслуживание и поиск неисправностей (по сравнению с шинной кабельной системой).
- надежность: изготовление компонентов и их сопровождение осуществляется одной фирмой, что обеспечивает повышенную надежность в эксплуатации.

С коннекторами компьютеры соединяются через ***сетевые адаптеры*** (Network Interfase Card – NIC).

NIC – это периферийное устройство компьютера, которое взаимодействует со средой ПД и связывает компьютер с другим (ми) компьютером (57отт).

Данные в NIC преобразуются в электромагнитные сигналы. NIC работает под управлением драйвера компьютера.

Между сетевыми адаптерами может устанавливаться специальное коммуникационное устройство (повторитель, концентратор, мост, коммутатор, маршрутизатор), которое берет на себя некоторые функции по управлению 57оттоком.

Функции сетевого адаптера:

- оформление передаваемой информации в виде кадра определенного формата;
- получение доступа к среде передачи данных (при использовании индивидуальных линий связи – установление соединения с коммутатором сети);
- кодирование последовательности бит кадра последовательностью электрических сигналов при передаче и декодирование при приеме;

- преодразование информации из параллельной формы в последовательную и наоборот;
- синхронизация битов, байтов и кадров.

Сетевые адаптеры разлчаются по типу и разрядности используемой в компьютере внутренней шины данных, по типу принятой в сети технологии (Ethernet? Token Ring? FDDI).

На рис.2.9 приведен пример схемы сетевого адаптера.

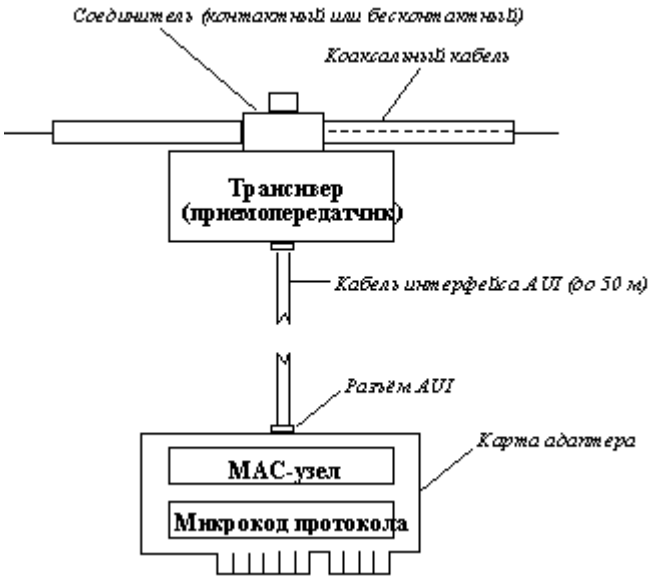


Рис. 2.9.. Структурная схема сетевого адаптера стандарта 10Base-5 («толстый» Ethernet)

27. Повторители и мосты

Простейшее из коммуникационных устройств - *повторитель (repeater)* - используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. Повторитель передает сигналы, приходящие из одного сегмента сети, в другие ее сегменты (рис. 1.14). Повторитель позволяет преодолеть ограничения на длину линий связи за счет улучшения качества передаваемого сигнала - восстановления его мощности и амплитуды, улучшения фронтов и т. п.

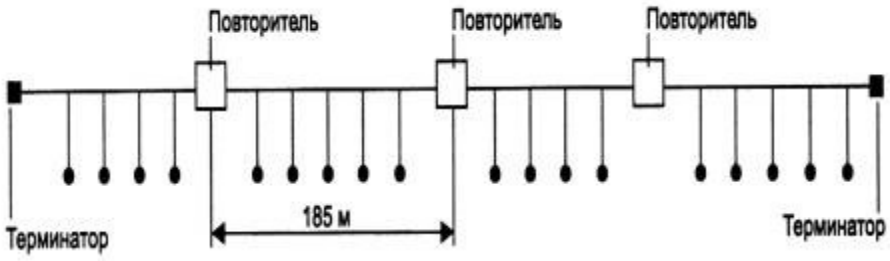


Рис. 1.14. Повторитель позволяет увеличить длину сети Ethernet

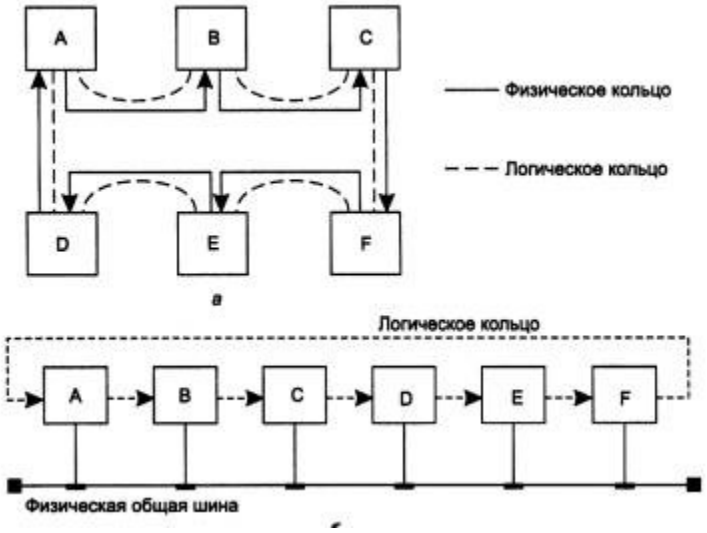


Рис. 1.16. Логическая и физическая топологии сети

Мост (bridge) делит разделяемую среду передачи сети на части (часто называемые логическими сегментами), передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если адрес компьютера назначения принадлежит другой подсети. Тем самым мост изолирует трафик одной подсети от трафика другой, повышая общую производительность передачи данных в сети. Локализация трафика не только экономит пропускную способность, но и уменьшает возможность несанкционированного доступа к данным, так как кадры не выходят за пределы своего сегмента и их сложнее перехватить злоумышленнику.

На рис. 1.18 показана сеть, которая была получена из сети с центральным концентратором (см. рис. 1.17) путем его замены на мост. Сети 1-го и 2-го отделов состоят из отдельных логических сегментов, а сеть отдела 3 - из двух логических сегментов. Каждый логический сегмент построен на базе концентратора и имеет простейшую физическую структуру, образованную отрезками кабеля, связывающими компьютеры с портами концентратора.

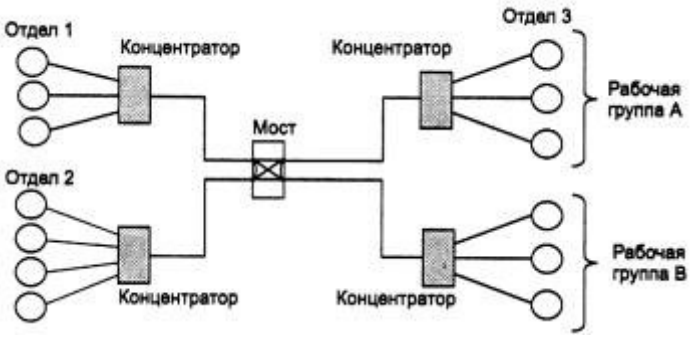


Рис. 1.18. Логическая структуризация сети с помощью моста

Мосты используют для локализации трафика аппаратные адреса компьютеров. Это затрудняет распознавание принадлежности того или иного компьютера к определенному логическому сегменту - сам адрес не содержит никакой информации по этому поводу. Поэтому мост достаточно упрощенно представляет деление сети на сегменты - он запоминает, через какой порт на него поступил кадр данных от каждого компьютера сети, и в дальнейшем передает кадры, предназначенные для этого компьютера, на этот порт. Точной топологии связей между логическими сегментами мост не знает. Из-за этого применение мостов приводит к значительным ограничениям на конфигурацию связей сети - сегменты должны быть соединены таким образом, чтобы в сети не образовывались замкнутые контуры.

28. Основы объединения сетей с помощью мостов

До недавнего времени единственным средством объединения сетей с различными протоколами канального уровня были маршрутизаторы. Однако в последнее время появилось много моделей мостов и коммутаторов, которые способны транслировать протоколы канального уровня локальных сетей. В связи с этим при необходимости объединения, например, сетей Ethernet и FDDI нет нужды ставить между этими сетями маршрутизатор, а можно воспользоваться более дешевым решением на основе транслирующего коммутатора.

По принципу передачи пакетов между сетями с разными канальными протоколами мосты и коммутаторы подразделяются на *инкапсулирующие* (encapsulating) и *транслирующие* (translational).

Инкапсулирующие мосты и коммутаторы

Инкапсулирующие мосты применяются тогда, когда необходимо соединить два сегмента сети, в которых используется один и тот же канальный протокол, через промежуточную сеть, использующую другой канальный протокол. При передаче данных мост упаковывает кадры первого сегмента в кадры промежуточного сегмента. Ясно, что максимальный размер инкапсулируемого кадра не должен превышать максимального размера поля данных кадра, в который он вкладывается.

После прохождения кадра по промежуточной части сети аналогичный мост удаляет оболочку промежуточного протокола и пакет продолжает свое движение в исходном виде. Очевидно, что при таком методе взаимодействие со станциями промежуточной сети невозможно, и эта сеть используется только как транзитное транспортное средство.

В виду широкого распространения другого класса мостов и коммутаторов, а именно транслирующих мостов и коммутаторов, инкапсуляция сейчас редко применяется для объединения локальных сетей с различными канальными протоколами.

Транслирующие мосты и коммутаторы

Транслирующие мосты и коммутаторы выполняют преобразование из одного протокола канального уровня в другой, например, Ethernet в FDDI, Fast Ethernet в Token Ring и т.п. Преобразование заключается в изменении формата кадра, в вычислении нового значения контрольной суммы.

Трансляцию протоколов канального уровня локальных сетей облегчает то обстоятельство, что наиболее сложную по трансляции адресной информации, в данном случае выполнять не нужно. Все конечные узлы локальных сетей имеют уникальные адреса одного и того же формата, независимо от поддерживаемого протокола. Поэтому адрес сетевого адаптера Ethernet понятен сетевому адаптеру FDDI, и они могут использовать эти адреса в полях своих кадров не задумываясь о том, что узел, с которым они взаимодействуют, принадлежит сети, работающей по другой технологии.

Единственным преобразованием, которое, возможно, придется выполнить, является преобразование порядка бит в байте, если согласуется сеть Ethernet с сетью Token Ring или FDDI. Это связано с тем, что в сетях Ethernet принята так называемая каноническая форма передачи адреса по сети, когда сначала передается самый младший бит самого старшего байта адреса. В сетях FDDI и Token Ring всегда передается сначала самый старший бит самого старшего байта адреса.

Кроме изменения порядка бит при передаче байт адреса, трансляция протокола Ethernet (и Fast Ethernet, который использует формат кадров Ethernet) в протоколы FDDI и Token Ring включает выполнение следующих (возможно не всех) операций:

- Вычисление длины поля данных кадра и помещение этого значения в поле Length при передаче кадра из сети FDDI или Token Ring в сеть Ethernet 802.3 (в кадрах FDDI и Token Ring поле длины отсутствует).
- Заполнение полей статуса кадра при передаче кадров из сети FDDI или Token Ring в сеть Ethernet. Кадры FDDI и Token Ring имеют два бита - бит распознавания адреса A и бит копирования кадра C.
- Отбрасывание кадров, передаваемых из сетей FDDI или Token Ring в сеть Ethernet с размером поля данных большим, чем 1500 байт, так как это максимально возможное значение поля данных для сетей Ethernet.
- Пересчет контрольной суммы кадра в соответствии со сформированными значениями служебных полей кадра.

Трансляция на уровне канальных протоколов имеет преимущества по сравнению с инкапсуляцией:

- меньше накладные расходы, так как не нужно передавать два заголовка канального уровня,
- доступность станций другой сети.

Но трансляция имеет и недостатки:

- транслирующие мосты и коммутаторы вносят дополнительную задержку при преобразовании форматов кадров, а также при новом вычислении контрольной суммы кадра,
- максимальный размер кадров у сетей, соединяемых транслирующими мостами и коммутаторами, должен быть одинаковым.

29. Хабы и коммутаторы

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов, часто называют концентратором, или хабом. Это отражает тот факт , что в данном устройстве сосредоточиваются все связи между сегментами сети.

Коммутатор (switch, switching hub) по принципу обработки кадров ничем не отличается от моста. Основное его отличие от моста состоит в том, что он является своего рода коммуникационным мультипроцессором, так как каждый его порт оснащен специализированным процессором, который обрабатывает кадры по алгоритму моста независимо от процессоров других портов. За счет этого общая производительность коммутатора обычно намного выше производительности традиционного моста, имеющего один процессорный блок. Можно сказать, что коммутаторы - это мосты нового поколения, которые обрабатывают кадры в параллельном режиме.

30. Схемные реализации коммутаторов ЛС-й

При построении небольших сетей, составляющих нижний уровень иерархии корпоративной сети, вопрос о применении того или иного коммуникационного устройства сводится к вопросу о выборе между концентратором или коммутатором.

При ответе на этот вопрос нужно принимать во внимание несколько факторов. Безусловно, немаловажное значение имеет стоимость в пересчете за порт, которую нужно заплатить при выборе устройства. Из технических соображений в первую очередь нужно принять во внимание существующее распределение трафика между узлами сети. Кроме того, нужно учитывать перспективы развития сети:

будут ли в скором времени применяться мультимедийные приложения, будет ли модернизироваться компьютерная база. Если да, то нужно уже сегодня обеспечить резервы по пропускной способности применяемого коммуникационного оборудования. Использование технологии intranet также ведет к увеличению объемов трафика, циркулирующего в сети, и это также необходимо учитывать при выборе устройства.

При выборе типа устройства - концентратор или коммутатор - нужно еще определить и тип протокола, который будут поддерживать его порты (или протоколов, если идет речь о коммутаторе, так как каждый порт может поддерживать отдельный протокол).

Сегодня выбор делается между протоколами трех скоростей - 10, 100 и 1000 Мбит/с. Поэтому, сравнивая применимость концентратора или коммутатора, необходимо рассмотреть варианты концентратора с портами на 10,100 и 1000 Мбит/с, а также несколько вариантов коммутаторов с различными комбинациями скоростей на портах.

Рассмотрим для примера вопрос о применимости коммутатора в сети с одним сервером и несколькими рабочими станциями, взаимодействующими только с сервером (рис. 4.43). Такая конфигурация сети часто встречается в сетях масштаба рабочей группы, особенно в сетях NetWare, где стандартные клиентские оболочки не могут взаимодействовать друг с другом.

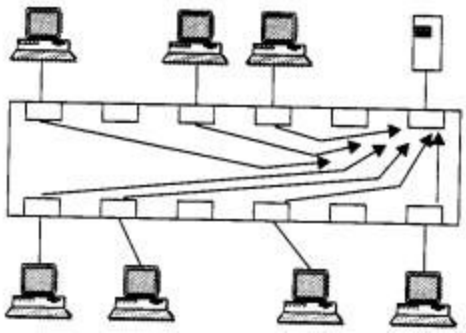


Рис. 4.43. Сеть с выделенным сервером

Если коммутатор имеет все порты с одинаковой пропускной способностью, например 10 Мбит/с, в этом случае пропускная способность порта в 10 Мбит/с будет распределяться между всеми компьютерами сети. Возможности коммутатора по повышению общей пропускной способности сети оказываются для такой конфигурации невостребованными. Несмотря на микросегментацию сети, ее пропускная способность ограничивается пропускной способностью протокола одного порта, как и в случае применения концентратора с портами 10 Мбит/с. Небольшой выигрыш при использовании коммутатора будет достигаться лишь за счет уменьшения количества коллизий - вместо коллизий кадры будут просто попадать в очередь к передатчику порта коммутатора, к которому подключен сервер.

Чтобы коммутатор работал в сетях с выделенным сервером более эффективно, производители коммутаторов выпускают модели с одним высокоскоростным портом на 100 Мбит/с для подключения сервера и несколькими низкоскоростными портами на 10 Мбит/с для подключения рабочих станций. В этом случае между рабочими станциями распределяется уже 100 Мбит/с, что позволяет обслуживать в неблокирующем режиме 10-30 станций в зависимости от интенсивности создаваемого ими трафика.

Однако с таким коммутатором может конкурировать концентратор, поддерживающий протокол с пропускной способностью 100 Мбит/с, например Fast Ethernet. Его стоимость в пересчете за порт будет несколько ниже стоимости за порт коммутатора с одним высокоскоростным портом, а производительность сети примерно та же.

Очевидно, что выбор коммуникационного устройства для сети с выделенным сервером достаточно сложен. Для принятия окончательного решения нужно принимать во внимание перспективы развития сети в отношении движения к сбалансированному трафику. Если в сети вскоре может появигься взаимодействие между рабочими станциями или же второй сервер, то выбор необходимо делать в пользу коммутатора, который сможет поддержать дополнительный трафик без ущерба по отношению к основному.

В пользу коммутатора можег сыграгь и фактор расстояний - применение коммутаторов не ограничиваег максимальный диаметр сети величинами в 2500 м или 210 м, которые определяют размеры домена коллизий при использовании концентраторов Ethernet и Fast Ethernet.

В целом существует тенденция постепенного вытеснения концентраторов коммутаторами, которая наблюдается примерно с 1996 года, который был назван весьма авторитетным журналом Data Communications «годом коммутаторов» в ежегодном прогнозе рынка сетевого оборудования.

Стянутая в точку магистраль на коммутаторе

При всем разнообразии структурных схем сетей, построенных на коммутаторах, все они используют две базовые структуры - стянутую в точку магистраль и распределенную магистраль. На основе этих базовых структур затем строятся разнообразные структуры конкретных сетей.

Стянутая в точку магистраль (collapsed backbone) - это структура, при которой объединение узлов, сегментов или сетей происходит на внутренней магистрали коммутатора. Пример сети рабочей группы такой структуры приведен на рис. 4.44.

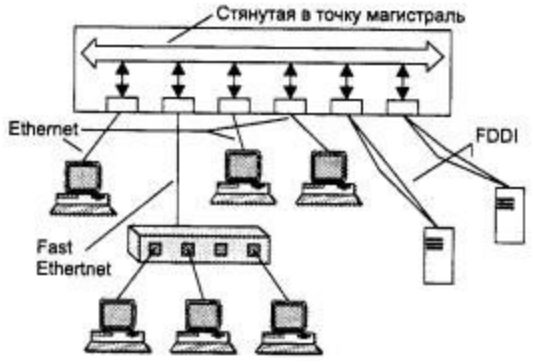


Рис. 4.44. Структура сети со стянутой в точку магистралью

Преимуществом такой структуры является высокая производительность магистрали. Так как для коммутатора производительность внутренней шины или схемы общей памяти, объединяющей модули портов, в несколько гигабит в секунду не является редкостью, то магистраль сети может быть весьма быстродействующей, причем ее скорость не зависит от применяемых в сети протоколов и может быть повышена с помощью замены одной модели коммутатора на другую.

Положительной чертой такой схемы является не только высокая скорость магистрали, но и ее протокольная независимость. На внутренней магистрали коммутатора в независимом формате одновременно могут передаваться данные различных протоколов, например Ethernet, FDDI и Fast Ethernet, как это изображено на рис. 4.44 Подключение нового узла с новым протоколом часто требует не замены коммутатора, а просто добавления соответствующего интерфейсного модуля, поддерживающего этот протокол.

Если к каждому порту коммутатора в такой схеме подключен только один узел, то такая схема будет соответствовать микросегментированной сети.

Распределенная магистраль на коммутаторах

В сетях больших зданий или кампусов структура с коллапсированной магистралью не всегда рациональна или возможна. Такая структура приводит к протяженным кабельным системам, связывающим конечные узлы или коммутаторы сетей рабочих групп с центральным коммутатором, шина которого и является магистралью сети. Высокая плотность кабелей и их высокая стоимость ограничивают применение стянутой в точку магистрали в таких сетях. Иногда, особенно в сетях кампусов, просто невозможно стянуть все кабели в одно помещение из-за ограничений на длину связей, накладываемых технологией (например, все реализации технологий локальных сетей на витой паре ограничивают протяженность кабелей в 100 м).

Поэтому в локальных сетях, покрывающих большие территории, часто используется другой вариант построения сети - с распределенной магистралью. Пример такой сети приведен на рис. 4.45.

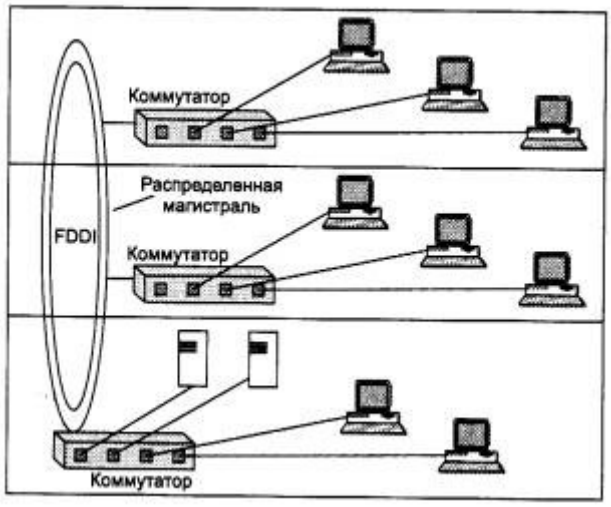


Рис. 4.45. Структура сети с распределенной магистралью

Распределенная магистраль - это разделяемый сегмент сети, поддерживающий определенный протокол, к которому присоединяются коммутаторы сетей рабочих групп и отделов. На примере распределенная магистраль построена на основе двойного кольца FDDI, к которому подключены коммутаторы этажей. Коммутаторы этажей имеют большое количество портов Ethernet, трафик которых транслируется в трафик протокола FDDI, когда он передается по магистрали с этажа на этаж.

Распределенная магистраль упрощает связи между этажами, сокращает стоимость кабельной системы и преодолевает ограничения на расстояния.

Однако скорость магистрали в этом случае будет существенно ниже скорости магистрали на внутренней шине коммутатора. Причем скорость эта фиксированная и в настоящее время чаще всего не превышает 100 Мбит/с. Поэтому распределенная магистраль может применяться только при невысокой интенсивности трафика между этажами или зданиями. Широкое распространение в недалеком будущем технологии Gigabit Ethernet может снять это ограничение, что очень положительно скажется на структуре крупных сетей.

Пример на рис. 4.45 демонстрирует сочетание двух базовых структур, так как на каждом этаже сеть построена с использованием магистрали на внутренней шине коммутатора.

31. Маршрутизаторы.

Ограничения, связанные с применением мостов и коммутаторов - по топологии связей, а также ряд других, - привели к тому, что в ряду коммуникационных устройств появился еще один тип оборудования - *маршрутизатор (router)*. Маршрутизаторы более надежно и более эффективно, чем мосты, изолируют трафик отдельных частей сети друг от друга. Маршрутизаторы образуют логические сегменты посредством явной адресации, поскольку используют не плоские аппаратные, а составные числовые адреса. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одному сегменту, называемому в данном случае *подсетью (subnet)*.

Кроме локализации трафика маршрутизаторы выполняют еще много других полезных функций. Так, маршрутизаторы могут работать в сети с замкнутыми контурами, при этом они осуществляют выбор наиболее рационального маршрута из нескольких возможных. Сеть, представленная на рис. 1.19, отличается от своей предшественницы (см. рис. 1.18) тем, что между подсетями отделов 1 и 2 проложена дополнительная связь, которая может использоваться как для повышения производительности сети, так и для повышения ее надежности.

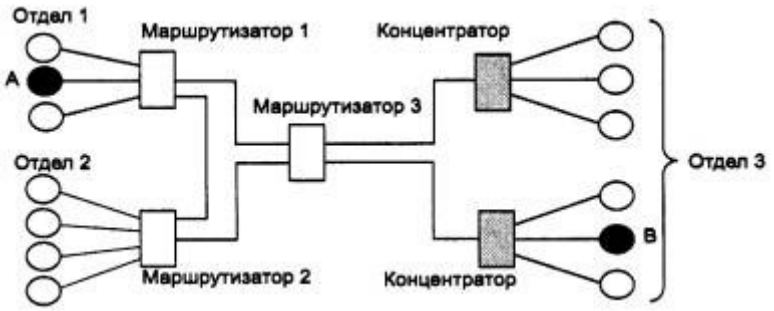


Рис. 1.19. Логическая структуризация сети с помощью маршрутизаторов

Другой очень важной функцией маршрутизаторов является их способность связывать в единую сеть подсети, построенные с использованием разных сетевых технологий, например Ethernet и X.25.

Кроме перечисленных устройств отдельные части сети может соединять *шлюз (gateway)*. Обычно основной причиной, по которой в сети используют шлюз, является необходимость объединить сети с разными типами системного и прикладного программного обеспечения, а не желание локализовать трафик. Тем не менее шлюз обеспечивает и локализацию трафика в качестве некоторого побочного эффекта.

Крупные сети практически никогда не строятся без логической структуризации. Для отдельных сегментов и подсетей характерны типовые однородные топологии базовых технологий, и для их объединения всегда используется оборудование, обеспечивающее локализацию трафика, - мосты, коммутаторы, маршрутизаторы и шлюзы.

Повторители, концентраторы, мосты, коммутаторы, маршрутизаторы и шлюзы

Мы уже успели в нашей книге рассмотреть множество способов доставки кадров и пакетов из одного сегмента кабеля в другой. Мы упоминали повторители, мосты, концентраторы, маршрутизаторы и шлюзы. Все эти устройства используются очень широко, однако в чем-то они различаются едва уловимо, а в чем-то весьма существенно. Число их весьма велико, поэтому лучше рассмотреть их все в совокупности, отмечая сходства и различия.

Надо начать с того, что эти устройства работают на разных уровнях, как показано на рис. 4.42, *а.* Это имеет значение, поскольку от этого зависит, какую часть информации устройство использует для маршрутизации. Типичный сценарий таков: у пользователя появляются какие-то данные, которые необходимо отправить на удаленную машину. Они передаются на транспортный уровень, который добавляет к ним свой заголовок (например, заголовок TCP) и передает результирующую единицу информации на сетевой уровень. Тот, в свою очередь, тоже добавляет свой заголовок, в результате чего формируется *пакет* сетевого уровня (например, IP-пакет). На рис. 4.42, *б* IP-пакет выделен серым цветом. Пакет отправляется на уровень передачи данных (канальный уровень), где обрастает еще одним заголовком и контрольной суммой (CRC). Наконец формируется кадр, который спускается на физический уровень и может быть передан, например, по ΛBC.

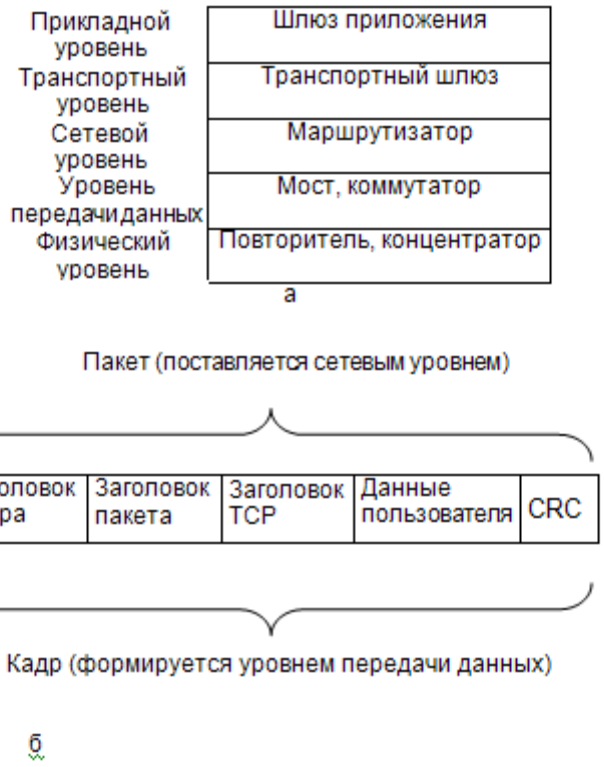
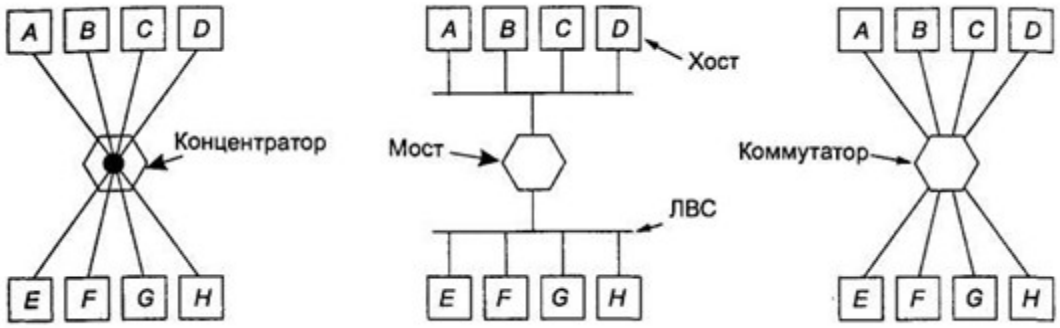


Рис. 4.42. Соответствие устройств уровням (а); кадры, пакеты и заголовки (б)

Приступим к рассмотрению коммутирующих устройств и взглянем на то, как они соотносятся с пакетами и кадрами. На самом нижнем, физическом уровне работают повторители. Это аналоговые устройства, к которым подсоединяются концы двух сегментов кабеля. Сигнал, появляющийся на одном из них, усиливается повторителем и выдается на второй. Повторители не знают слов «пакет», «кадр» или «заголовок». Они знают слово «напряжение». В классическом Ethernet допускается установка четырех повторителей, что позволяет расширять максимальную длину кабеля с 500 до 2500 м.

Теперь обратимся к концентраторам. Концентратор (хаб) имеет несколько входов, объединяемых электрически. Кадры, прибывающие на какой-либо вход, передаются на все остальные линии. Если одновременно по разным линиям придут два кадра, они столкнутся, как в коаксиальном кабеле. То есть концентратор представляет собой одну область столкновений. Все линии, подсоединяемые к нему. должны работать с одинаковыми скоростями. Концентраторы отличаются от повторителей тем, что они обычно не усиливают входные сигналы, поскольку предназначены не для этого. Их задача — обеспечивать согласованную работу нескольких плат с несколькими входами, к которым подключаются линии с похожими параметрами. Впрочем, во всем остальном хабы не очень отличаются от повторителей. Ни те, ни другие не анализируют и не используют адреса стандарта 802. Принцип работы концентратора показан на рис. 4.43, *а.*



а б в

Рис.4.43. Концентратор (а); мост (б); коммутатор (в)

Перейдем теперь на уровень передачи данных. Здесь мы обнаружим мосты и коммутаторы. Только что мы как раз более или менее подробно обсуждали мосты, поэтому знаем, что мост соединяет две или более ЛВС, как показано на рис. 4.43, *б.* Когда прибывает кадр, мост программно извлекает из заголовка и анализирует адрес назначения, сопоставляя его с таблицей и определяя, куда этот кадр должен быть передан. В Ethernet это 48-битный адрес, показанный на рис. 4.16. Как и в концентраторах, в современных мостах имеются вставные сетевые платы, обычно рассчитанные на 4 или 8 входов определенного типа. Плата Ethernet, например, не может обрабатывать кадры сетей типа маркерное кольцо, поскольку она не знает, в какой части заголовка искать адрес назначения. Тем не менее, мост может иметь несколько плат, благодаря чему может работать с сетями разных типов. Каждая линия, подключенная к мосту, является областью столкновений, в отличие от линий концентратора.

Коммутаторы похожи на мосты в том, что для маршрутизации используют адреса кадров. На самом деле многие употребляют эти понятия как синонимы. Различаются они тем, что коммутаторы чаще всего используются для соединения отдельных компьютеров (рис. 4.43, *в),* а не сетей. Следовательно, если хост *А* (рис. 4.43, *б)* хочет отправить кадр на хост *В,* мост получит этот кадр, но отвергнет его. Вместе с тем, коммутатор на рис. 4.43, *в* должен самым активным образом способствовать передаче кадра от хоста *А* к хосту *В,* поскольку для кадра это единственная возможность. Так как каждый порт коммутатора обычно соединен с одним компьютером, в коммутаторах должно быть гораздо больше разъемов Для сетевых плат, чем в мостах, поскольку последние соединяют целые сети. Каждая плата содержит буфер для хранения пришедших кадров. Поскольку каждый порт является областью столкновений, то кадры из-за коллизий теряться не могут. Однако если скорость передачи данных по каналу превысит максимальную скорость их обработки, буфер может переполниться и продолжающие приходить кадры будут отвергаться.

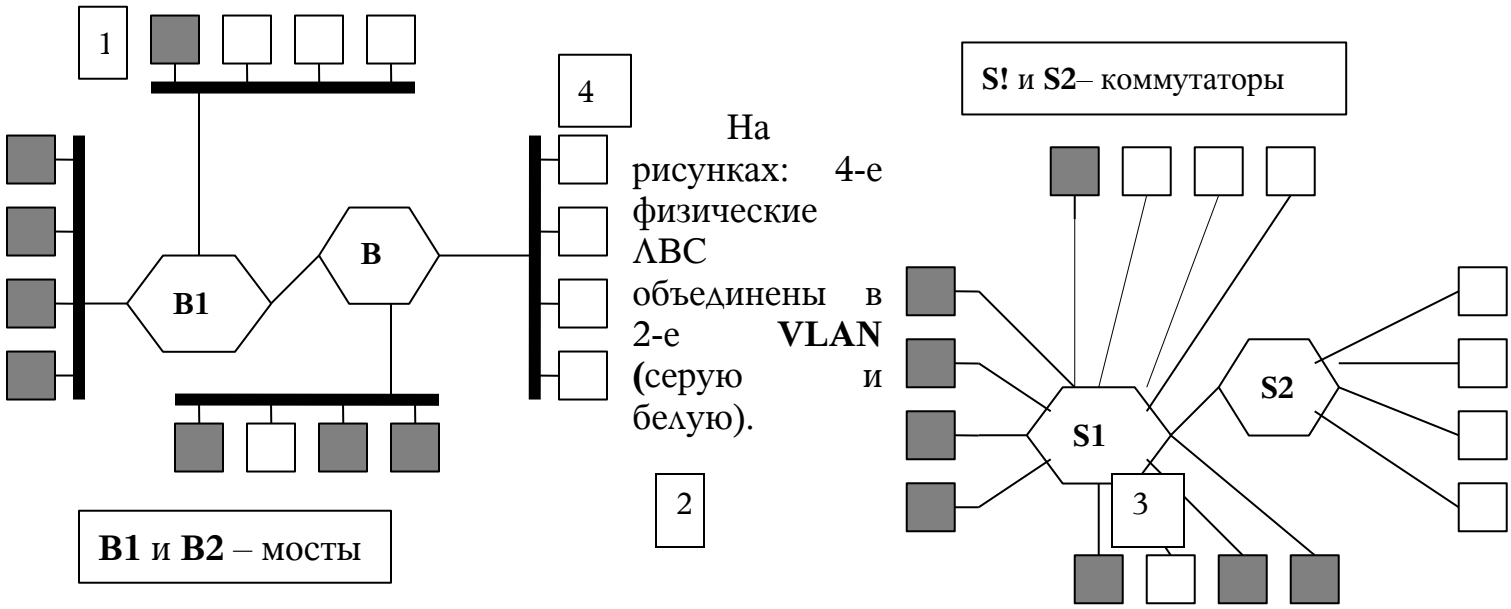
Несколько уменьшить эту проблему помогают современные коммутаторы, которые начинают пересылать кадры, едва получив их заголовки и не дожидаясь полной их докачки (конечно, для этого должна быть свободна выходная линия). Такие коммутаторы не используют протоколы с ожиданием. Иногда их называют сквозными коммутаторами. Этот метод чаще всего реализуется аппаратно, тогда как в мостах традиционно присутствует процессор, программно реализующий маршрутизацию с ожиданием. Но поскольку все современные мосты и коммутаторы содержат специальные интегральные схемы коммутации, техническая разница между ними практически стирается, и остается лишь разница в том, что вы слышите о них в рекламе.

Итак, мы вкратце рассмотрели повторители и концентраторы, которые весьма сходны друг с другом, а также коммутаторы и мосты, которые также не сильно различаются. Теперь же мы перейдем к маршрутизаторам, которые резко отличаются от всего рассмотренного ранее. Когда пакет прибывает на маршрутизатор, отрезаются заголовки и концевики кадров и остаются только поля данных (выделены серым на рис. 4.42), которые и передаются программному обеспечению маршрутизатора. Далее анализируется заголовок пакета, и в соответствии с ним выбирается его дальнейший путь. Если это IP-пакет, то в заголовке будет содержаться 32-битный (IPv4) или 128-битный (IPv6), а не 48-битный (стандарт 802) адрес. Программное обеспечение маршрутизатора не интересуется адресами кадров и даже не знает, откуда эти кадры взялись (то ли с ЛВС, то ли с двухточечной линии). Более подробно мы изучим маршрутизаторы и принципы маршрутизации в главе 5.

Поднявшись еще на уровень выше, мы обнаружим транспортные шлюзы. Они служат для соединения компьютеров, использующих различные транспортные протоколы, ориентированные на установление соединения. Например, такая ситуация возникает, когда компьютеру, использующему TCP/IP, необходимо передать данные компьютеру, использующему ATM. Транспортный шлюз может копировать пакеты, одновременно приводя их к нужному формату.

Наконец, шлюзы приложений уже работают с форматами и содержимым пакетов, занимаясь переформатированием на более высоком уровне. Например, шлюз e-mail может переводить электронные письма в формат SMS-сообщений для мобильных телефонов

32. Виртуальные локальные сети



На рисунках: 4-е физические ЛВС объединены в 2-е **VLAN** (серую и белую).

Коммутатор позволяет локализовывать потоки информации в сети, контролировать эти потоки и управлять ими, используя пользовательские фильтры.

Однако пользовательский фильтр может запретить передачи кадров только по конкретным адресам, а широковещательный трафик он передает всем сегментам сети. Так требует алгоритм работы моста, который реализован в коммутаторе, поэтому сети, созданные на основе мостов и коммутаторов иногда называют плоскими - из-за отсутствия барьеров на пути широковещательного трафика. Технология виртуальных сетей (Virtual LAN, VLAN) позволяет преодолеть указанное ограничение.

Виртуальной сетью называется группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сегментами на основании адреса канального уровня невозможна, независимо от типа адреса - уникального, группового или широковещательного.

В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра.

Назначение технологии виртуальных сетей состоит в облегчении процесса создания независимых сетей, которые затем должны связываться с помощью протоколов сетевого уровня.

При использовании технологии виртуальных сетей в коммутаторах одновременно решаются две задачи:

- повышение производительности в каждой из виртуальных сетей, так как коммутатор передает кадры в такой сети только узлу назначения;
- изоляция сетей друг от друга для управления правами доступа пользователей и создания защитных барьеров на пути широковещательных штормов.

При изменении состава сегментов (переход пользователя в другую сеть, дробление крупных сегментов) приходится производить физическую перекоммутацию разъемов на передних панелях повторителей или в кроссовых панелях, что не очень удобно в больших сетях - много физической работы, к тому же высока вероятность ошибки.

В VLAN приписывание отдельного порта к любому из внутренних сегментов производится программным путем. Программное приписывание порта сегменту часто называют статической или конфигурационной коммутацией.

Чтобы VLAN функционировали корректно, необходимо наличие *конфигурационных таблиц* в мостах и коммутаторах. Таблицы сообщают, через какие порты производится доступ к тем или иным VLAN.

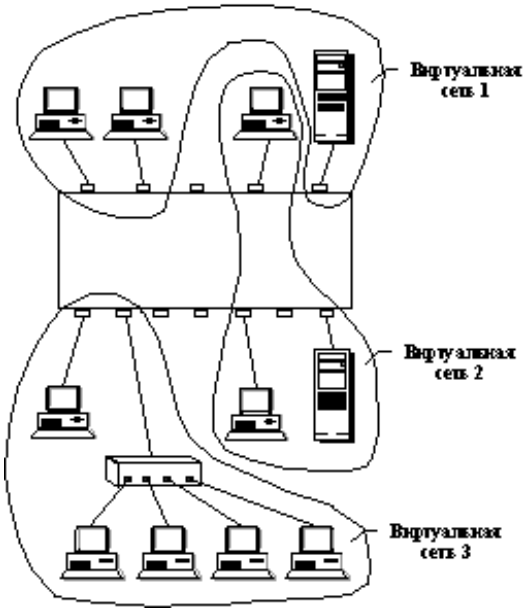
Когда кадр прибывает из «серой» ЛВС, его нужно разослать на все порты, помеченные таким же цветом. Как мосты и коммутаторы «узнают» «цвет» приходящего кадра?

Существует несколько способов построения виртуальных сетей:
- Группировка портов.
- Группировка MAC-адресов.
- Все протоколы 3-го уровня или IP-адреса соответствуют определенному цвету (содержание кадра).

VLAN на основе группировки портов

При создании виртуальных сетей на основе одного коммутатора обычно используется механизм группирования в виртуальные сети портов коммутатора.

Это логично, так как виртуальных сетей, построенных на основе одного коммутатора, не может быть больше, чем портов. Если к одному порту подключен сегмент, построенный на основе повторителя, то узлы такого сегмента не имеет смысла включать в разные виртуальные сети - все равно трафик этих узлов будет общим.



Виртуальные сети, построенные на одном коммутаторе с помощью группировки портов

Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы - достаточно каждый порт приписать к нескольким заранее поименованным

виртуальным сетям. Обычно, такая операция выполняется путем перетаскивания мышью графических символов портов на графические символы сетей.

VLAN на основе группировки MAC-адресов

Второй способ, который используется для образования виртуальных сетей основан на группировании MAC-адресов.

Мост или коммутатор имеет таблицу, в которой представлены 48-битовый адреса и названия VLAN всех станций, соединенных с устройством.

Можно смешивать VLAN-ы в одной физической сети.

Когда прибывает кадр, мост или коммутатор извлекают из него MAC-адрес и находят его в , что позволяет определить в какой VLAN находится станция с этим MAC-адресом.

VLAN на основе содержания кадра

Мост (коммутатор) просматривает поле данных кадров, чтобы классифицировать машины с IP-адресами к одной VLAN, а машины с Apple-Talk – к другой VLAN. Такая стратегия полезна особенно, когда часть машин представляют собой НОУТБУКИ, которые могут подключаться в разных местах).

Но есть проблема: такой подход нарушает фундаментальный закон сетей – *независимость уровней.*

Уровню передачи данных не должнобыть никакого дела до содержимого поля данных. Тем более, чтобы по нему принимать решения.

Решение проблемы: предложен **стандарт 802.1Q**

Если бы была возможность VLAN по заголовку кадра, то отпала бы необходимость анализировать содержание кадра.

Но в Ethernet нет запасных полей.

Комитет IEEE 802 изменил формат заголовка кадра Ethernet.

Новый формат под именем 802.1Q был опубликован в 1998 г.

Формат Ethernet 802.3 включает поля (в последовательности слева на право): адрес получателя, адрес отправителя, длина, данные, наполнитель, контрольная сумма. Лимит длины кадра Ethernet – 1518 байт.

Новый стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети.

Стандарт IEEE 802.1p специфицирует метод указания приоритета кадра, основанный на использовании новых полей, определенных в стандарте IEEE 802.1Q.

К кадру Ethernet добавлены два байта. Эти 16 бит содержат информацию по принадлежности кадра Ethernet к VLAN и о его приоритете. Тремя битами кодируется до восьми уровней приоритета, 12 бит позволяют различать трафик до 4096 VLAN, а один бит зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet.

Длина кадра в стандарте 802.1Q решается путем повышения лимита: вместо 1518 – 1522 байта.

Резюме: виртуальные ЛВС (VLAN) обеспечивают возможность создания логических групп пользователей в масштабе корпоративной сети. За счет использования VLAN администратор сети может организовать пользователей в **логические** группы независимо от **физического** расположения рабочих станций этих пользователей. Это одно **из основных достижений** в сетевых технологиях - возможность создавать рабочие группы на основе служебных функций пользователей, не привязываясь к сетевой топологии. Виртуальные сети позволяют организовать работу в сети более эффективно.

Виртуальные сети обеспечивают целый ряд преимуществ:

- простота внесения изменений в сеть, добавления или удаления устройств;
- более эффективное использование ограниченных сетевых ресурсов;
- высокий уровень обеспечения безопасности.

Возможность организации виртуальных ЛВС обусловлена переходом от разделяемых сред к коммутируемым.

33. Беспроводные ЛС

Несмотря на то, что Ethernet чрезвычайно популярен, ему все же есть с кем соперничать. Беспроводные локальные вычислительные сети становятся все более популярными, все больше и больше офисных зданий, аэровокзалов и других общественных мест оборудуются соответствующей аппаратурой. Беспроводные ЛВС могут существовать в двух конфигурациях: с базовой станцией и без нее. Стандарт 802.11 принимает это во внимание и поддерживает оба варианта. Далее мы вкратце рассмотрим данный стандарт.

Собственно говоря, мы уже касались вопроса беспроводных ЛВС в главе 1, разделе «Ethernet». Теперь более пристальный взгляд обратим на технологическую сторону стандарта 802.11. В последующих разделах речь пойдет о стеке протоколов, методах радиопередачи (на физическом уровне), протоколе подуровня MAC, структуре кадра и сервисах. Дополнительную информацию о стандарте 802.11 можно найти в следующих изданиях (Crow и др., 1997; Geier, 2002; Heegar и др., 2001; Kapp, 2002; O'Hara и Petrick, 1999; Serevance, 1999). Чтобы получить информацию из первых рук, обратитесь к официальному техническому описанию стандарта.

Стандарт 802.11: стек протоколов

Все протоколы, используемые семейством стандартов 802.x, схожи по структуре. Часть стека протоколов изображена на рис. 4.22. Физический уровень практически соответствует физическому уровню в модели OSI, а вот уровень передачи Данных во всех протоколах 802.x разбит на два или более подуровня. Что касается 802.11, то подуровень MAC (подуровень управления доступом к среде) отвечает за распределение канала, то есть за то, какая станция будет передавать следующей. Над MAC в иерархии находится подуровень LLC (управления логическим соединением), задача которого состоит в том, чтобы сделать различия стандартов 802.x невидимыми для сетевого уровня. Мы уже рассматривали LLC ранее, когда речь шла об Ethernet, поэтому сейчас мы не будем возвращаться к этому материалу.

Рис.4.22. Часть стеков протокола 802

Стандарт 802.11 1997 года определяет три метода передачи, реализуемые на физическом уровне. Метод инфракрасной передачи сильно напоминает метод, используемый в системах дистанционного

управления бытовой техникой. В двух других методах применяется радиосвязь небольшого радиуса действия (при этом работают методы FHSS и DSSS). Они оба используют не подлежащую лицензированию часть спектра (диапазон ISM 2,4 ГГц). В этой же части спектра осуществляют передачу сигнала радиобрелоки открывания ворот гаражей, так что не удивляйтесь, если ваш ноутбук не сможет в какой-то момент поделить эфир с вашим же гаражом. Кроме того, в этом же диапазоне работают домашние радиотелефоны и СВЧ-печи. Вне зависимости от метода скорость работы составляет 1-2 Мбит/с, и сигнал используется относительно маломощный, что позволяет уменьшить количество конфликтов между передатчиками. С целью увеличения пропускной способности в 1999 году были разработаны два дополнительных метода: OFDM и HR-DSSS. Они работают со скоростями 54 Мбит/с и 11 Мбит/с соответственно. В 2001 году была представлена новая модификация OFDM, работающая в другом частотном диапазоне. Сейчас мы изучим вкратце все эти методы. Они относятся к физическому уровню, которому была посвящена, вообще говоря, вся глава 2. Но из-за того, что они так тесно связаны с ЛВС вообще и с подуровнем MAC стандарта 802.11 в частности, мы обращаемся к ним здесь.

Стандарт 802.11: физический уровень

Все пять рассматриваемых далее методов передачи данных позволяют передать кадр подуровня MAC с одной станции на другую. Различаются они используемыми технологиями и достижимыми скоростями. Детальное рассмотрение этих методов выходит за рамки данной книги, мы лишь дадим краткое описание, которое, возможно, заинтересует читателей и снабдит их необходимыми терминами для поиска более подробной информации в Интернете или где-то еще.

При передаче в инфракрасном диапазоне (вне диапазона видимого света) используются длины волн 0,85 или 0,95 мкм. Возможны две скорости передачи: 1 и 2 Мбит/с. При 1 Мбит/с используется схема кодирования с группировкой четырех бит в 16-битное кодовое слово, содержащее 15 нулей и 1 единицу. Это так называемый код Грея. Одно из его свойств заключается в том, что небольшая ошибка в синхронизации может привести в худшем случае к ошибке в одном бите выходной последовательности. При скорости передачи 2 Мбит/с уже 2 бита кодируются в 4-битное кодовое слово, также имеющее всего одну единицу: 0001, 0010, 0100 или 1000. Сигналы инфракрасного диапазона не проникают сквозь стены, поэтому соты, расположенные в разных комнатах, очень хорошо изолированы друг от друга. Однако из-за довольно низкой пропускной способности (а также потому, что солнечный свет может искажать инфракрасные сигналы) этот метод не слишком популярен.

В методе FHSS (Frequency Hopping Spread Spectrum — передача широкополосных сигналов по методу частотных скачков) используются 79 каналов шириной 1 МГц каждый. Диапазон, в котором работает этот метод, начинается с 2,4 ГГц (это нелицензируемый [ISM] диапазон). Для определения последовательностей скачков частот используется генератор псевдослучайных чисел. Поскольку при этом для всех станций используется один и тот же генератор, они синхронизированы во времени и одновременно осуществляют одинаковые частотные скачки. Период времени, в течение которого станция работает на определенной частоте, называется временем пребывания. Это настраиваемая величина, но она должна быть не более 400 мс. Рандомизация, осуществляемая в методе FHSS, является простым способом распределения неуправляемого ISM-диапазона. Кроме того, постоянная смена частот — это неплохой (хотя, конечно, недостаточный) способ защиты информации от несанкционированного прослушивания, поскольку незваный слушатель, не зная последовательности частотных переходов и времени пребывания, не сможет подслушать передаваемые данные. При связи на более Длинных дистанциях может возникать проблема многолучевого затухания, и FHSS может оказаться хорошим подспорьем в борьбе с ней. Этот метод также относительно слабо чувствителен к интерференции с радиосигналом, что делает его популярным при связи между зданиями. Главный недостаток FHSS — это низкая пропускная способность.

Третий метод модуляции называется DSSS (Direct Sequence Spread Spectrum — передача широкополосного сигнала по методу прямой последовательности). Скорости передачи ограничены 1 или 2 Мбит/с. DSSS немного напоминает Уже обсуждавшуюся в разделе «Второе поколение мобильных телефонов: цифровая передача голоса» систему CDMA, однако имеет и некоторые отличия. Каждый бит передается в виде 11 элементарных сигналов, которые называются последовательностью Баркера. Для

этого используется модуляция с фазовым сдвигом со скоростью 1 Мбод (1 бит на бод при работе на 1 Мбит/с и 2 бита на бод при работе на 2 Мбит/с). В течение нескольких лет комиссия FCC требовала, чтобы все беспроводное оборудование в США работало в нелицензируемых диапазонах, однако в мае 2002 года это требование было снято, поскольку появились новые технологии.

Первая высокоскоростная беспроводная ЛВС, **802.11a,** использовала метод **OFDM** (Orthogonal Frequency Division Multiplexing — ортогональное частотное уплотнение) для передачи сигнала со скоростью до 54 Мбит/с в расширенном нелицензируемом диапазоне 5 ГГц. Как и полагается при частотном уплотнении, здесь используются разные частоты. Всего их 52, из них 48 частот предназначены для данных, 4 — для синхронизации (почти как в ADSL). Одновременная передача сигналов на разных частотах позволяет говорить о расширенном спектре, хотя этот метод существенно отличается от CDMA и FHSS. Разделение сигнала на много узких диапазонов имеет преимущества перед передачей в одном широком диапазоне — в частности, более низкую чувствительность к узкополосной интерференции и возможность использования независимых диапазонов. Система кодирования довольно сложна. Она основана на модуляции с фазовым сдвигом для скоростей до 18 Мбит/с и на QAM при более высоких скоростях. При 54 Мбит/с 216 бит данных кодируются 288-битными кодовыми словами. Одним из преимуществ OFDM является совместимость с европейской системой HiperLAN/2 (Doufexi и др., 2002). Метод имеет хорошую спектральную эффективность в терминах соотношения бит/герц и хороший иммунитет против многолучевого затухания.

Наконец, мы подошли к методу **HR-DSSS** (High Rate Direct Sequence Spread Spectrum — высокоскоростная передача широкополосного сигнала по методу прямой последовательности). Это еще один широкополосный способ, который для достижения скорости 11 Мбит/с кодирует биты со скоростью 11 миллионов элементарных сигналов в секунду. Стандарт называется **802.11b,** но он не является последователем 802.11a. На самом деле 802.11b был признан и попал на рынок даже раньше, чем 802.11a. Скорости передачи данных, поддерживаемые этим стандартом, равны 1, 2, 5,5 и И Мбит/с. Две низкие скорости требуют 1 Мбод при 1 и 2 битах на бод соответственно. Используется модуляция с фазовым сдвигом (для совместимости с DSSS). Две высокие скорости требуют кодирования со скоростью 1,375 Мбод при 4 и 8 битах на бод соответственно. Применяется **код Уолша — Адамара.** Скорость передачи может быть динамически изменена во время работы для достижения оптимальных результатов в зависимости от условий нагрузки и зашумленности линии. На практике скорость работы стандарта 802.11b почти всегда равна 11 Мбит/с. Хотя 802.11b медленнее, чем 802.11a, диапазон первого почти в 7 раз шире, что бывает очень важно во многих ситуациях.

Улучшенная версия 802.11b называется **802.llg.** Этот стандарт был принят IEEE в ноябре 2001 года после долгих обсуждений того, чья же патентованная технология будет применяться. В итоге в 802.llg применяется метод модуляции OFDM, взятый из 802.11a, однако рабочий диапазон совпадает с 802.11b (узкий нелицензированный диапазон 2,4 ГГц). Теоретически максимальная скорость 802.1 lg равна 54 Мбит/с. До сих пор не очень понятно, может ли быть достигнута такая скорость на практике. Зато, пока суть да дело, комитет 802.11 может гордо заявить, что он разработал три высокоскоростных стандарта беспроводных ЛВС: 802.11a, 802.11b и 802.11g (не говоря уж о трех низкоскоростных беспроводных ЛВС). Можно вполне обоснованно удивляться тому, что же в этом хорошего. Ну, видимо, три — это просто счастливое число для комитета 802.11.

Стандарт 802.11: протокол подуровня управления доступом к среде

Однако вернемся из области электротехники в область computer science. Протокол подуровня MAC (напомним, MAC расшифровывается как Medium Access Control — управление доступом к среде) в стандарте 802.11 довольно сильно отличается от аналогичного протокола Ethernet благодаря присущей беспроводным сетям сложности по сравнению с проводными сетями. В Ethernet станция просто ожидает, пока в канале настанет тишина, и тогда начинает передачу. Если шумовой всплеск не приходит обратно в течение времени, необходимого на пересылку 64 байт, то можно утверждать, что кадр почти наверняка доставлен корректно. В беспроводных сетях такой фокус не проходит.

Во-первых, существует проблема скрытой станции — мы уже упоминали о ней ранее, а сейчас приводим еще и иллюстрацию (рис. 4.23, с). Поскольку не все станции могут слышать друг друга, передача, идущая в одной части соты, может быть просто не воспринята станцией, находящейся в другой ее части. В приведенном на рисунке примере станция *C* передает данные станции *B*. Если станция *A* прослушает канал, она не обнаружит ничего подозрительного и сделает ложный вывод о том, что она имеет право начать передачу станции *B*. Кроме того, есть и обратная проблема, показанная на рис. 4.23, *б*. Здесь *B* хочет отправить данные для станции *C* и прослушивает канал. Услышав, что в нем уже осуществляется какая-то передача, станция *B* делает опять-таки ложный вывод о том, что передача для *C* сейчас невозможна. Между тем станция *A* — источник сигнала, который смутил станцию *B,* — может на самом деле осуществлять передачу для станции *D* (на рисунке не показана). Ситуация усугубляется еще и тем, что большинство радиосистем являются полудуплексными, то есть не могут одновременно и на одной и той же частоте посылать сигналы и воспринимать всплески шума на линии. В итоге 802.11 не может использовать, как Ethernet, метод CSMA/CD.

Как бороться с этой проблемой? Стандарт 802.11 поддерживает два режима работы. Первый называется **DCF** (Distributed Coordination Function — распределенная координация) и не имеет никаких средств централизованного управления (в этом смысле напоминая Ethernet). Второй режим, **PCF** (Point Coordination Function — сосредоточенная координация), подразумевает, что базовая станция берет на себя функцию управления активностью всех станций данной соты. Все реализации стандарта должны поддерживать DCF, тогда как PCF является дополнительной возможностью. Сейчас мы перейдем к рассмотрению этих режимов.

В режиме DCF 802.11 использует протокол, называемый CSMA/CA (CSMA with Collision Avoidance — CSMA с предотвращением коллизий). Здесь ведется прослушивание как физического, так и виртуального канала. Протокол CSMA/CA может работать в двух режимах. В первом режиме станция перед передачей прослушивает канал. Если он свободен, начинается пересылка данных. Во время пересылки канал не прослушивается, и станция передает кадр целиком, причем он может быть разрушен на стороне приемника из-за интерференции сигналов. Если канал занят, отправитель дожидается его освобождения и затем начинает передачу. Если возникает коллизия, станции, не поделившие между собой
канал,

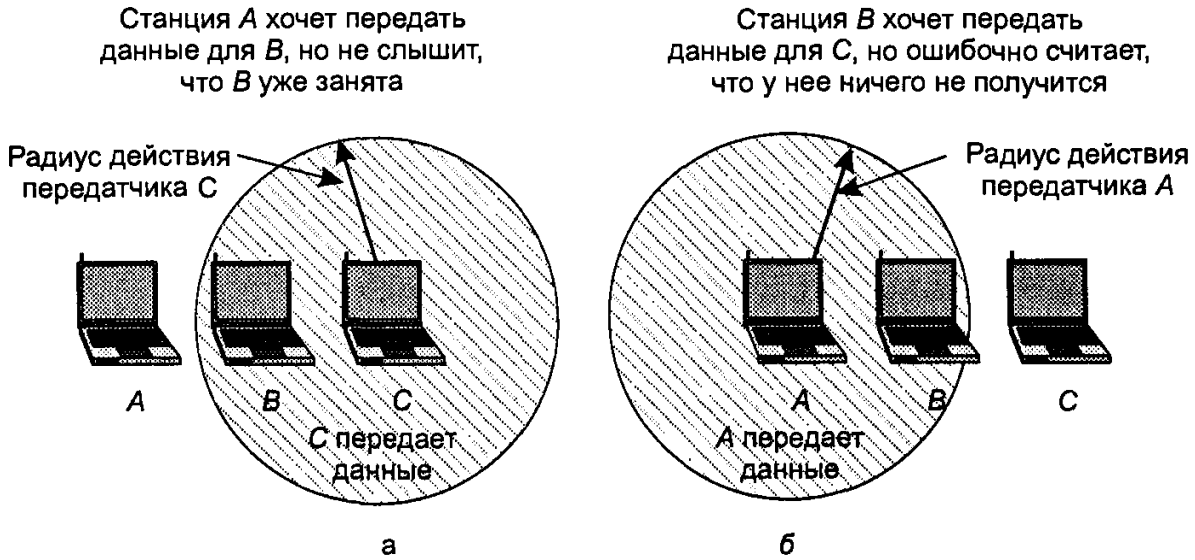


Рис. 4.23. Проблема скрытой станции (*а*); проблема засвеченной станции (*б*)

выжидают в течение случайных интервалов времени (используется двоичный экспоненциальный откат такой же, как в Ethernet) и затем снова пытаются отправить кадр.

Другой режим CSMA/CA основан на протоколе MACAW и использует контроль виртуального канала, как показано на рис. 4.24. В этом примере станция *A* хочет передать данные станции *B*. Станция

C находится в зоне действия (то есть слышит) *A,* а также, возможно, в зоне действия *B,* но это не имеет значения. Станция *D* входит в зону действия *B,* но не входит в зону действия *A.*

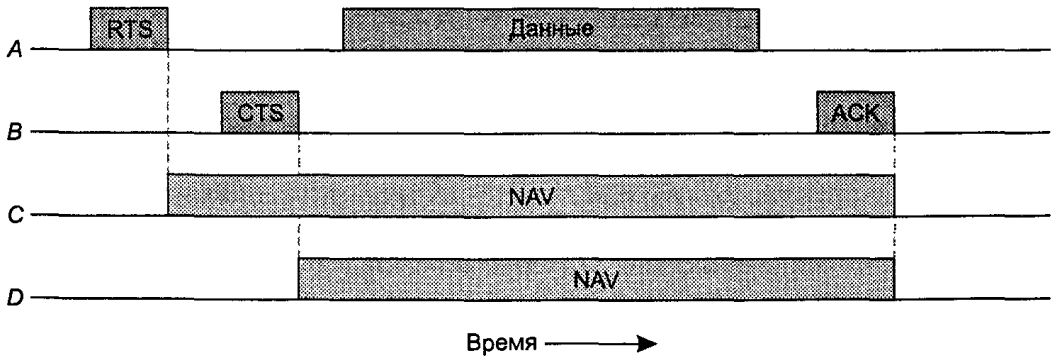


Рис. 4.24. Использование прослушивания виртуального канала в протоколе CSMA/CA

Протокол начинает работать тогда, когда *A* решает, что ей необходимо послать данные *B*. *A* посылает станции *B* кадр RTS, запрашивая разрешение на передачу. Если *B* может принять данные, она отсылает обратно положительное подтверждение, кадр CTS. После приема CTS *A* запускает таймер ACK и начинает передачу данных. В случае корректного приема *B* генерирует кадр ACK, сообщающий станции *A* о конце передачи. Если интервал времени таймера на станции *A* истекает прежде, чем получен ACK, весь алгоритм работы протокола повторяется с самого начала.

Теперь рассмотрим этот же процесс с точки зрения станций *C* и *D*. *C* находится в зоне действия *A,* поэтому она также принимает кадр RTS и понимает, что скоро по каналу будут передаваться какие-то данные и лучше при этом помолчать и подождать окончания активности соседних станций. Исходя из информации, содержащейся в RTS, станция *C* может предположить, сколько времени займет передача последовательности, включая конечный ACK. В течение этого промежутка *C* считает, что ее виртуальный канал занят и она может отдыхать. Индикацией такого состояния является последовательность NAV (Network Allocation Vector — вектор выделенной сети), показанная на рис. 4.24. Станция *D* не слышит RTS, посылаемый *A,* зато слышит CTS, посланный станцией *B,* и также выставляет NAV. Обратите внимание: сигналы NAV не передаются, а являются лишь внутренними напоминаниями станций о том, что нужно хранить молчание в течение определенного промежутка времени.

В противоположность проводным каналам, беспроводные шумны и ненадежны, в какой-то степени из-за СВЧ-печей, работающих в том же диапазоне. В результате вероятность корректной передачи кадра уменьшается пропорционально увеличению длины кадра. Если вероятность ошибки в одном бите равна *p,* то вероятность того, что n-битный кадр будет принят корректно, равна $(1 - p)^n$. Например, для $p = 10^{-4}$ вероятность корректной передачи полного Ethernet-кадра длиной 12 144 бит составляет менее 30 %. Если $p = 10^{-5}$, примерно один кадр из 9 будет испорчен. Даже при $p = 10^{-6}$ более 1 % кадров будет испорчено, то есть за 1 секунду ошибки в кадрах будут возникать примерно 12 раз. Длинные кадры вообще имеют очень мало шансов дойти до получателя неповрежденными, и их нужно посылать заново.

Для решения проблемы зашумленных каналов беспроводных сетей применяется разбиение кадров на небольшие отрезки, каждый из которых содержит собственную контрольную сумму. Фрагменты нумеруются и подтверждаются индивидуально с использованием протокола с ожиданием (то есть отправитель не может передать фрагмент с номером $k + 1$, пока не получит подтверждения о доставке фрагмента с номером k). Захватив канал с помощью диалога, состоящего из RTS и CTS, отправитель может передать несколько кадров подряд, как показано на рис. 4.25. Последовательность фрагментов называется пачкой фрагментов.

Фрагментация повышает производительность путем принудительной повторной пересылки коротких отрезков кадров, в которых произошла ошибка, а не кадров целиком. Размер фрагмента не закрепляется стандартом, а является настраиваемым параметром каждой ячейки беспроводной сети и может оптимизироваться базовой станцией. Механизм выставления NAV удерживает станции от передачи только до прихода первого подтверждения о доставке. Но есть и другой.

Широкополосные беспроводные сети

Что-то мы засиделись в помещении. Выйдем на улицу и посмотрим — может быть, там тоже есть какие-нибудь интересные сети? А там действительно что-то есть, и в основном мы увидим то, что называется «последней милей». Во многих странах телефонная система в какой-то момент перестала быть жестко управляемой, и появилось множество фирм, предлагающих локальные услуги голосовой связи и интернет-услуги.

Предложений действительно много. Проблема только в том, что прокладка волоконно-оптического кабеля, коаксиала или даже витой пары пятой категории к миллионам абонентов обходится очень дорого. Что же делать?

Ответ одновременно и прост, и сложен. Нужны широкополосные беспроводные сети. Установить одну большую антенну на горке где-нибудь рядом с населенным пунктом и расставить на крышах домов абонентов приемные антенны гораздо проще и дешевле, чем рыть траншеи и протягивать кабель. Таким образом, конкурирующие операторы связи оказались крайне заинтересованы в развитии многомегабитных беспроводных систем связи, реализующих услуги голосовой коммуникации, доступа к Интернету, видео по заказу и т. д. Как было продемонстрировано на рис. 2.27, очень неплохо с задачей справляется система LMDS. Однако еще до недавних пор каждый оператор стремился использовать свою собственную систему. Отсутствие стандартов означало, что аппаратное и программное обеспечение не могли быть запущены в массовое производство. Это, в свою очередь, приводило к установке неоправданно высоких цен при низкой популярности.

Наконец светлые головы, работающие в данной отрасли, поняли, что именно стандартизация широкополосных беспроводных сетей является главным камнем Преткновения. По традиции, сформировать комитет для разработки стандарта было поручено IEEE. В комитет 802.16 вошли представители крупнейших фирм и научных организаций. Работа была начата в июле 1999 года, а официальный результат был представлен в апреле 2002 года. Название стандарта таково: "Эфирный интерфейс стационарных широкополосных беспроводных систем Доступа». Тем не менее, большинство предпочитает использовать более короткое название: беспроводные региональные сети, или беспроводные местные линии. М*ы* считаем, что все эти названия равноценны и взаимозаменяемы. - Подобно некоторым другим стандартам из серии 802, стандарт 802.16 построен с использованием идей модели OSI. Здесь можно найти и уровни, и подуровни, используется схожая терминология, сервисные примитивы и т. п. К сожалению, как и OSI, стандарт 802.16 страдает громоздкостью. В последующих Разделах мы приведем краткое описание основных его свойств, но такое исследование является далеко не полным, в нем опущены многие детали. Дополнительную общую информацию о широкополосных беспроводных сетях вы найдете в (Bolcskei и др., 2001; Webb, 2001). Информацию о конкретном стандарте 802.16 можно найти в (Eklund и др., 2002).

Сравнение стандартов 802.11 и 802.16

Казалось бы, зачем провозглашать новый стандарт? Чем так плохи сети 802.11, что их нельзя уж и на улицу вынести? Объяснений появлению нового стандарта можно найти несколько. Во-первых, 802.11 и 802.16 решают совершенно разные проблемы. Прежде чем говорить о каких-либо технических подробностях, стоит, наверное, сказать несколько слов в защиту создателей именно нового стандарта.

Сети 802.11 и 802.16 похожи друг на друга прежде всего в том, что и те, и другие предназначены для обеспечения беспроводной связи с высокой пропускной способностью. Однако дальше начинаются различия. Во-первых, 802.16 предоставляет услуги связи для целых зданий, а здания, как известно, отличаются крайне малой мобильностью. Они не часто мигрируют из соты в соту. Между тем сети 802.11 во многом ориентированы на мобильность абонентов. В здании может быть расположено несколько

компьютеров, и этот вариант несколько сложнее, чем мобильная станция с единственным ноутбуком. Владельцы зданий обычно готовы платить за хорошую связь больше, чем владельцы ноутбуков, поэтому появляется возможность установки качественных радиоприемников и передатчиков. В частности, этот аспект влияет на то, что сеть 802.16 может использовать полнодуплексную связь, тогда как экономия денег пользователями сети 802.11 не дает такой возможности.

Сети 802.16 могут охватывать целые районы городов, и расстояния при этом исчисляются километрами. Следовательно, получаемый станциями сигнал может быть разной мощности в зависимости от их удаленности от передатчика. Эти отклонения влияют на соотношение сигнал/шум, что, в свою очередь, приводит к использованию нескольких схем модуляции. Этот вид телекоммуникаций является открытым, эфирный сигнал проходит над целыми городами, поэтому вопросы защиты информации здесь крайне важны.

В каждой ячейке широкополосной региональной сети может быть намного больше пользователей, чем в обычной ячейке 802.11, и при этом каждому пользователю предоставляется гораздо более высокая пропускная способность, чем пользователю беспроводной ЛВС. Кроме всего прочего, трудно представить себе, чтобы начальство фирмы собрало в одной комнате офисного здания 50 сотрудников, для того чтобы посмотреть, что будет с сетью, если на каждую из 50 мобильных станций загружать свой видеофильм. В среде пользователей 802.16 такая ситуация может легко возникнуть сама собой, только не в пределах одной комнаты, а в пределах одной ячейки региональной сети. Нелицензированной (ISM) полосы частот явно недостаточно для такой нагрузки, поэтому сети 802.16 работают в высокочастотном диапазоне 10-66 ГГц. На момент разработки стандарта это была единственная подходящая незанятая часть спектра.

Но ведь миллиметровые волны такого диапазона обладают совсем иными физическими свойствами, чем более длинные волны ISM-диапазона. Значит, необходимо разработать специальный физический уровень для 802.16. Миллиметровые волны, увы, очень эффективно поглощаются водой (особенно дождем, снегом, градом, а иногда даже туманом). Значит, нужно как-то это учитывать при обработке ошибок. Данный тип волн является узконаправленным (волны, применяемые в стандарте 802.11, распространяются по всем направлениям), поэтому вопрос о многолучевом распространении здесь становится больше теоретическим, чем практическим.

Еще одна проблема — качество обслуживания. Сети 802.11 поддерживают передачу информации в реальном времени (в режиме PCF), но вообще-то они не предназначены для телефонной связи и большого мультимедийного трафика. Стандарт 802.16, напротив, ориентирован на поддержку подобных приложений, поскольку он предназначен как для обывателей, так и для деловых людей.

В двух словах можно так обрисовать различие между описываемыми сетями: стандарт 802.11 — это мобильный аналог Ethernet, а 802.16 — беспроводной, но стационарный аналог кабельного телевидения. Разница оказалась столь большой, что стандарты получились совсем не похожие. Это и понятно: они служат разным целям.

Можно попробовать провести некую аналогию с сотовой телефонной системой. Говоря о мобильных телефонах, мы подразумеваем голосовую связь, осуществляемую в довольно узком частотном диапазоне, с невысокой мощностью и волнами средней длины. Никто (пока что) не смотрит на экранах мобильных телефонов двухчасовые фильмы с высоким разрешением. Даже UMTS, похоже, не Изменит ситуацию. Короче говоря, запросы у пользователей беспроводных региональных сетей гораздо выше, чем у владельцев мобильных аппаратов. Следовательно, нужна совсем другая система. Вопрос о возможном использовании стандарта 802.16 для мобильных приложений остается открытым. Он не подразумевает этого, но такая возможность, в принципе, есть. На сегодняшний день ведется беспроводное обслуживание исключительно стационарных абонентов.

Стандарт 802.16: стек протоколов

Набор протоколов, используемый стандартом 802.16, показан на рис. 4.28. Общая структура подобна другим стандартам серии 802, однако здесь мы видим больше Подуровней. Нижний подуровень занимается физической передачей данных. Ис-Пользуется обычная узкополосная радиосистема с обыкновенными схемами модуляции сигнала. Над физическим уровнем находится подуровень сведения (с ударением на второй слог), скрывающий от уровня передачи данных различия технологий. На самом деле, в стандарте 802.11 можно найти нечто подобное, просто комитет не потрудился дать этому название в стиле модели OSI.

Хотя мы и не показали этого на рисунке, уже разрабатываются два новых протокола физического уровня. Стандарт 802.16а будет поддерживать OFDM в диапазоне 2-11 ГГц. 802.16b сможет работать в 5-гигагерцевом ISM-диапазоне. Обе вариации на тему 802.16 представляют собой попытки приблизиться к 802.11.

Уровень передачи данных состоит из трех подуровней. Нижний из них относится к защите информации, что очень критично для сетей, в которых передача данных осуществляется в эфире, физически никак не защищенном от прослушивания. В сетях 802.11 в прямом смысле слова «стены помогают» скрыть информацию от несанкционированного доступа. На этом подуровне производится шифрация, дешифрация данных, а также управления ключами доступа.

Для достижения этой цели можно установить на каждой сети по мосту и соединить эти мосты линиями «точка — точка» (например, арендованными у телефонной компании линиями). Простая система из трех локальных сетей показана на рис. 4.41. К данной конструкции применим обычный алгоритм маршрутизации. Проще всего рассматривать три двухточечные линии как локальную сеть без хостов. Нигде до сих пор не утверждалось, что в локальной сети обязательно должны быть хосты.

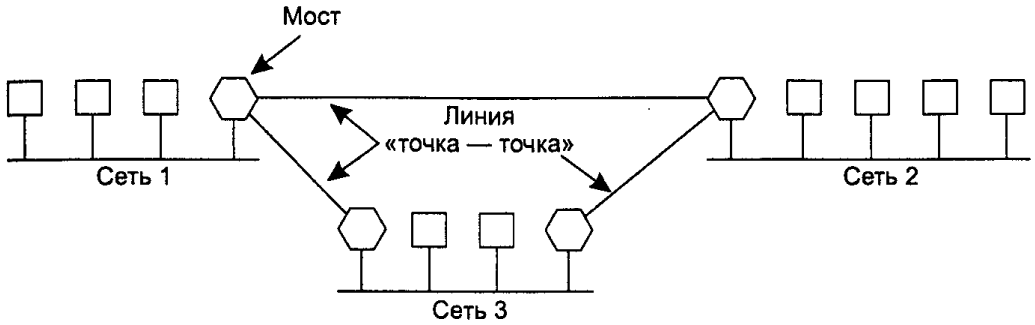


Рис. 4.41. Для соединения дальних сетей можно использовать удаленные хосты

На двухточечных линиях могут использоваться различные протоколы. Одним из вариантов может быть выбор какого-либо стандартного двухточечного протокола передачи данных с помещением кадров уровня доступа к носителю (MAC) целиком в поле данных. Такая стратегия наиболее оправданна в том случае, когда сети идентичны, при этом единственной проблемой остается доставка кадров в правильную сеть. Другой вариант заключается в том, что у кадров уровня доступа к носителю на первом мосту удаляются заголовок и концевик и в поле полезной нагрузки протокола «точка — точка» помещается то, что осталось. На втором мосту заголовок и концевик уровня доступа к носителю создаются заново. Недостаток такого метода состоит в том, что контрольная сумма по дороге несколько раз пересчитывается заново, что увеличивает вероятность появления не обнаруженных ошибок.

34. Телекоммуникационные сети с КК, КС, КП

С точки зрения среднего телефонного инженера, телефонная система состоит из двух частей: внешнего оборудования (местных телефонных линий и магистралей, вне коммутаторов) и внутреннего оборудования (коммутаторов), расположенного на телефонной станции. Мы рассмотрели внешнее оборудование. Теперь пора уделить внимание внутреннему.

В телефонных системах используются два различных приема: коммутации каналов и коммутации пакетов. Далее мы кратко познакомимся с каждым из них. Затем мы несколько подробнее обсудим коммутацию каналов, поскольку именно в соответствии с этой схемой функционирует современная телефонная система. Коммутацию пакетов мы изучим более детально в последующих главах.

Коммутация каналов

Когда вы (или ваш компьютер) снимаете телефонную трубку и набираете номер, коммутирующее оборудование телефонной системы отыскивает физический путь, состоящий из кабелей (медных или оптоволоконных; впрочем, это может быть и радиоканал) и ведущий от вашего телефона к телефону того, с кем вы связываетесь. Такая система, называемая коммутацией каналов, схематически изображена на рис. 2.33, *а.* Каждый из шести прямоугольников представляет собой коммутирующую станцию (оконечную или междугородную). В данном примере каждая станция имеет три входных и три выходных линии. Когда звонок проходит через коммутационную станцию, между входной и выходной линиями устанавливается физическое соединение, как показано пунктирными линиями (такова, по крайней мере, концепция).

На заре телефонии соединение устанавливалось вручную телефонным оператором, который замыкал две линии проводом с двумя штекерами на концах. С изобретением автоматического коммутатора связана довольно забавная история. Автоматический коммутатор изобрел в XIX веке владелец похоронного бюро Алмон Б. Строуджер (Almon B. Strowger) вскоре после изобретения телефона. Когда кто-либо умирал, родственник умершего звонил городскому телефонному оператору и говорил: «Соедините меня, пожалуйста, с похоронным бюро». К несчастью для мистера Строуджера, в его городе было два похоронных бюро, и жена владельца конкурирующей фирмы как раз работала телефонным оператором. Мистер Строуджер быстро понял, что либо он изобретет автоматический телефонный коммутатор, либо ему придется закрывать дело. Он выбрал первое. На протяжении почти 100 лет используемое во всем мире оборудование для коммутации каналов называлось искателем Строуджера. (История не упоминает, не устроилась ли жена его конкурента, уволенная с работы телефонного оператора, в телефонное справочное агентство, сообщая телефонный номер своего похоронного бюро всем желающим.)

Модель, изображенная на рис. 2.33, *а,* конечно, сильно упрощена, поскольку канал, соединяющий двух абонентов телефонной линии, на самом деле может быть не только медным проводом, но и, например, микроволновой или оптоволоконной магистралью, на которой объединены тысячи телефонных абонентов. Тем не менее, основная идея остается той же самой: когда один абонент звонит другому, устанавливается определенный путь, связывающий их, и этот путь остается неизменным до конца разговора.

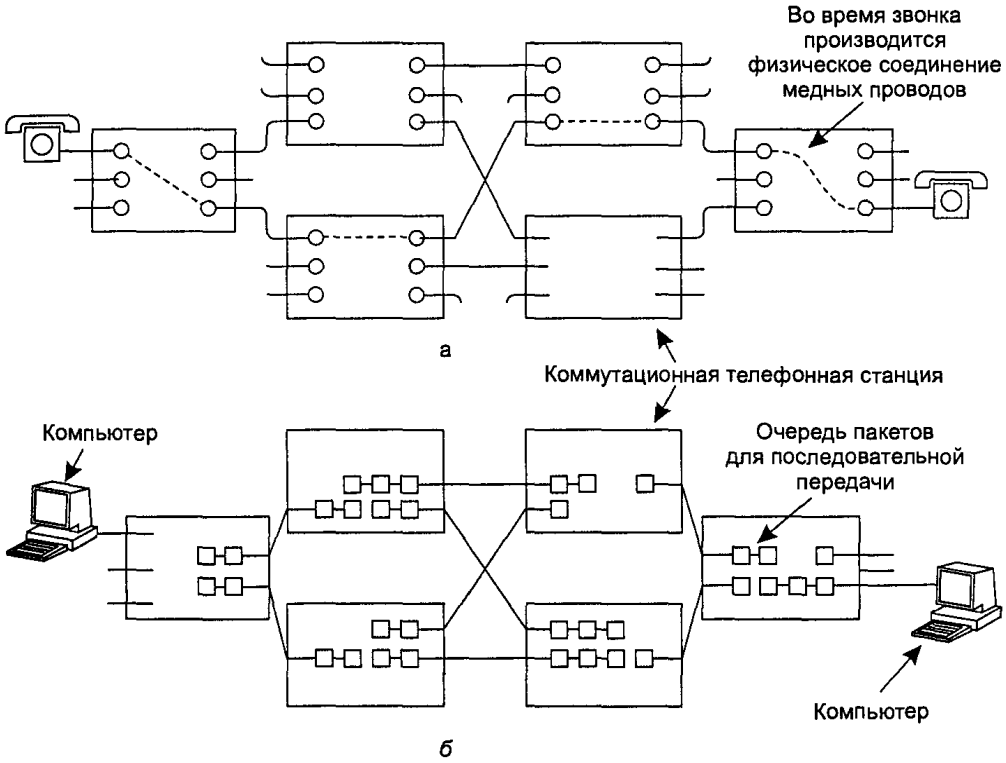


Рис. 2.33. Коммутация кеналов (*а*); коммутация пакетов (*б*)

Альтернативным способом коммутации является коммутация пакетов, которая схематически изображена на рис. 2.33, *б*. Отдельные пакеты пересылаются как положено, однако заранее никакой путь между абонентами не устанавливается. Каждый пакет должен сам искать свой путь.

Важным свойством коммутации каналов является необходимость установления сквозного пути от одного абонента до другого *до* того, как будут посланы данные. Именно поэтому время от конца набора номера до начала разговора может занимать около 10 с и более для междугородных или международных звонков. В течение этого интервала времени телефонная система ищет путь, изображенный на рис. 2.33, *а*. Обратите внимание на то, что еще до начала передачи данных сигнал запроса на разговор должен пройти весь путь до пункта назначения и должен там быть распознан. Для многих компьютерных приложений (например, при проверке кредитной карточки клиента кассовым терминалом) длительное время установления связи является нежелательным.

В результате при установлении физического соединения между абонентами, как только этот путь установлен, единственной задержкой для распространения сигнала будет скорость распространения электромагнитного сигнала, то есть около 5 мс на каждые 1000 км. Еще одним свойством такой системы является то, что после начала разговора линия уже не может вдруг оказаться занятой, хотя она может быть занятой до установки соединения (например, благодаря отсутствию соответствующей возможности у коммутатора или магистрали).

Коммутация сообщений

Еще одной стратегией является **коммутация сообщений,** показанная на рис. 2.34, *б*. При использовании такой формы коммутации физический путь между абонентами заранее не устанавливается. Вместо этого, когда отправитель желает отослать данные, они сохраняются на ближайшей коммутационной станции (то есть на первом маршрутизаторе), а затем прыжками от одного маршрутизатора к другому передаются дальше. Каждый блок принимается целиком, анализируется на наличие ошибок, после чего пересылается дальше. В сетях такой прием называется **передачей с промежуточным хранением,** об этом уже рассказывалось в главе 1.

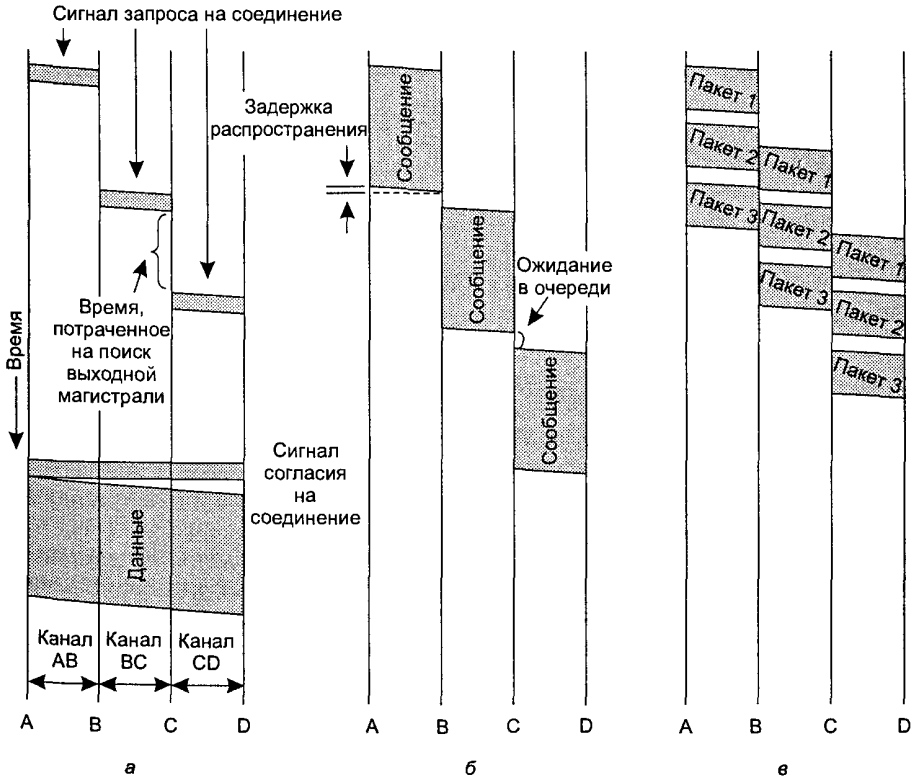


Рис. 2.34. Синхронизация событий при коммутации: каналов (*а*); сообщений (*б*); пакетов (*а*)

Коммутация сообщений использовалась в первой электромагнитной системе связи, а именно в телеграфе. Телеграмма печаталась на бумажной ленте в отключенном от линии режиме на станции-отправителе, а затем прочитывалась с ленты и передавалась по линии связи на следующую станцию, где она снова пробивалась на бумажной ленте. Оператор отрывал ленту от мотка и читал ее на одном из нескольких специальных устройств чтения лент, которых было столько же, сколько исходящих магистралей. Такой коммутатор назывался конторой рваных лент (torn tape office). Бумажные ленты уже далеко в прошлом, коммутация сообщений больше не используется, поэтому мы больше не будем затрагивать эту тему.

Коммутация пакетов

При коммутации сообщений размер блоков никак не ограничивается. Это означает, что маршрутизаторы (в современных системах) должны быть оснащены дисками для буферизации длинных блоков. Это также означает, что один блок может занять линию, связывающую два маршрутизатора, на несколько минут. В целом, система коммутации сообщений плохо подходит для интерактивного трафика. Данная проблема решилась, когда был изобретен метод коммутации пакетов, который мы уже упоминали в главе 1. В сетях с коммутацией пакетов на размер блоков накладывается жесткое ограничение, что позволяет буферизировать блоки не на диске, а в памяти маршрутизатора. Сети с коммутацией пакетов удовлетворяют требованиям интерактивного трафика, поскольку ни один пользователь не может монополизировать линию на длительное время (измеряемое миллисекундами). Еще одно преимущество коммутации пакетов перед коммутацией сообщений продемонстрировано на рис. 2.34, *б и в:* первый пакет многопакетного сообщения пересылается еще до того, как второй пакет полностью получен, что уменьшает задержку и повышает скорость передачи. По этим причинам компьютерные сети обычно используют систему коммутации пакетов, иногда — коммутацию каналов, но никогда не применяют коммутацию сообщений.

Коммутация каналов отличается от коммутации пакетов по ряду факторов. Во-первых, при коммутации каналов связь между двумя абонентами должна быть установлена до начала передачи данных. Пакетная коммутация такого требования не предъявляет. Первый пакет отсылается, как только он появляется.

Результатом предварительной установки соединения при коммутации каналов является резервирование всей пропускной способности для конкретного сеанса. Все пакеты следуют установленным путем. Кроме всего прочего, это означает, что пакеты не могут прийти в неправильной последовательности. При коммутации пакетов единого пути для них не существует, они могут приходить независимо друг от друга по пути, определяемому состоянием сети в момент передачи. Соответственно, не исключено, что пакеты придут в неправильном порядке.

Пакетная коммутация более устойчива к сбоям. На самом деле, именно это свойство стало причиной изобретения данного метода. Если, например, выходит из строя один из коммутаторов, то все линии, подключенные к нему, также выходят из строя. Но при коммутации пакетов данные могут быть отправлены в обход «умершего» коммутатора.

Предварительное установление соединения дает возможность предварительно зарезервировать полосу пропускания. В этом случае при получении пакета его можно мгновенно переслать дальше. При коммутации пакетов полоса пропускания не резервируется, поэтому могут возникать очереди из пакетов, ожидающих пересылки.

Если полоса пропускания резервируется заранее, на линии не может возникнуть затор (если только не пытаться послать больше пакетов, чем ожидается). С другой стороны, сама попытка установить предварительное соединение может оказаться неудачной из-за перегрузки канала. То есть ситуация перегрузки в разных методах может возникать в разное время: при коммутации пакетов такое может случиться при передаче данных, а при коммутации каналов — при установлении соединения.

Если определенная линия уже зарезервирована для какого-то соединения, но по ней ничего не передается, то она простаивает. Ею не могут воспользоваться другие абоненты. При коммутации пакетов линия не простаивает, а значит, такой метод является более эффективным с точки зрения всей системы. Понимание того, чем приходится жертвовать в каждом из этих методов, необходимо, чтобы ощутить разницу между пакетной коммутацией и коммутацией каналов. В любом случае ищется какой-то компромисс между гарантией качества обслуживания при больших затратах ресурсов и отсутствием гарантии качества при малых затратах ресурсов.

Коммутация пакетов использует передачу с промежуточным хранением. Пакет сохраняется в памяти маршрутизатора, после чего пересылается дальше. При коммутации каналов биты просто непрерывной чередой следуют по линии связи. Промежуточное сохранение пакетов вносит задержки в процесс передачи.

Еще одним отличием является то, что коммутация каналов абсолютно прозрачна для пользователей. Отправитель и получатель могут использовать любую скорость передачи, любой формат данных или метод формирования кадров. Транспортная часть системы ничего не знает об этих подробностях и даже не интересуется ими. При коммутации пакетов транспортная служба определяет основные параметры. Можно привести довольно грубое сравнение с различием между шоссе и железной дорогой. При движении по шоссе пользователь сам определяет скорость, размер и тип автомобиля. При перемещении по железной дороге подобные вопросы решаются специальной службой. Благодаря такой прозрачности системы передавать голос, данные и факсы в телефонной системе можно одновременно.

Наконец, еще одним различием между двумя способами коммутации является политика оплаты услуг. Системы с коммутацией каналов традиционно взимают плату за расстояние передачи и время на линии. В мобильных телефонах расстояние роли не играет (кроме международных звонков), а время играет не очень значительную роль (ну, например, тариф с 2000 бесплатных минут дороже, чем тариф с 1000 бесплатных минут, причем иногда звонки в ночное время и в выходные являются льготными). В случае коммутации пакетов время на линии вообще не принимается в расчет, однако иногда взимается плата за трафик. С обычных пользователей провайдеры иногда берут просто ежемесячную абонентскую плату, поскольку это проще для обеих сторон, однако магистральные транспортные службы взимают с местных провайдеров плату за объем трафика. Все различия сведены в табл. 2.5.

Таблица 2.5. Сравнительные характеристики коммутации каналов и коммутации пакетов

Параметр	Коммутация каналов	Коммутация пакетов
Установка соединения	Требуется	Не требуется
Выделенный «медный» путь	Да	Нет
Каждый пакет перемещается по одному и тому же пути	Да	Нет
Пакеты приходят в правильном порядке	Да	Нет
Критичность выхода из строя коммутатора	Да	Нет
Доступная пропускная способность	Фиксированная	Динамическая
Возможность занятости линии	Во время установки соединения	Для каждого пакета
Возможность простоя линии	Да	Нет
Передача с промежуточным хранением	Нет	Да
Прозрачность	Да	Нет
Оплата	За время на линии	За трафик

36. Принцип КП с использованием техники ВК-в

Описанный выше режим передачи пакетов между двумя конечными узлами сети предполагает независимую маршрутизацию каждого пакета. Такой режим работы сети называется дейтаграммным, и при его использовании коммутатор может изменить маршрут какого-либо пакета в зависимости от состояния сети — работоспособности каналов и других коммутаторов, длины очередей пакетов в соседних коммутаторах и т. п.

Существует и другой режим работы сети — передача пакетов *по виртуальному каналу (virtual circuit* или *virtual channel).* В этом случае перед тем, как начать передачу данных между двумя конечными узлами, должен быть установлен виртуальный канал, который представляет собой единственный маршрут, соединяющий эти конечные узлы. Виртуальный канал может быть динамическим или постоянным. Динамический виртуальный канал устанавливается при передаче в сеть специального пакета — запроса на установление соединения. Этот пакет проходит через коммутаторы и «прокладывает» виртуальный канал. Это означает, что коммутаторы запоминают маршрут для данного соединения и при поступлений последующих пакетов данного соединения отправляют их всегда по проложенному маршруту. Постоянные виртуальные каналы создаются администраторами сети путем ручной настройки коммутаторов.

При отказе коммутатора или канала на пути виртуального канала соединение разрывается, и виртуальный канал нужно прокладывать заново. При этом он, естественно, обойдет отказавшие участки сети.

Каждый режим передачи пакетов имеет свои преимущества и недостатки. Дейтаграммный метод не требует предварительного установления соединения и поэтому работает без задержки перед передачей данных. Это особенно выгодно для передачи небольшого объема данных, когда время установления соединения может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстрее адаптируется к изменениям в сети.

Пои использовании метола виптуальных каналов время, затраченное на установление виртуального канала, компенсируется последующей быстрой передачей всего потока пакетов. Коммутаторы распознают принадлежность пакета к виртуальному каналу по специальной метке - номеру виртуального канала, а не анализируют адреса конечных узлов, как это делается при дейтаграммном методе.

37. Стек протоколов TCP/IP.

В стеке TCP/IP определены 4 уровня (рис. 5.5). Каждый из этих уровней несет на себе некоторую нагрузку по решению основной задачи - организации надежной и производительной работы составной сети, части которой построены на основе разных сетевых технологий.

Уровень I	Прикладной уровень
Уровень II	Основной (транспортный) уровень
Уровень III	Уровень межсетевого взаимодействия
Уровень IV	Уровень сетевых интерфейсов

Рис. 5.5. Многоуровневая архитектура стека TCP/IP

Уровень межсетевого взаимодействия

Стержнем всей архитектуры является *уровень межсетевого взаимодействия,* который реализует концепцию передачи пакетов в режиме без установления соединений, то есть дейтаграммным способом. Именно этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональным. Этот уровень также называют уровнем internet, указывая тем самым на основную его функцию - передачу данных через составную сеть.

Основным протоколом сетевого уровня (в терминах модели OSI) в стеке является протокол IP (Internet Protocol). Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Так как протокол IP является дейтаграммным протоколом, он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Основной уровень

Поскольку на сетевом уровне не устанавливаются соединения, то нет никаких гарантий, что все пакеты будут доставлены в место назначения целыми и невредимыми или придут в том же порядке, в котором они были отправлены. Эту задачу -обеспечение надежной информационной связи между двумя конечными узлами -решает *основной уровень* стека TCP/IP, называемый также *транспортным*.

На этом уровне функционируют протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений. Этот протокол позволяет равноранговым объектам на компьютере-отправителе и компьютере-получателе поддерживать обмен данными в дуплексном режиме. TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток байт в любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части - *сегменты,* и передает их ниже лежащему уровню межсетевого взаимодействия. После того как эти сегменты будут доставлены средствами уровня межсетевого взаимодействия в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и главный протокол уровня межсетевого взаимодействия IP, и выполняет только функции связующего звена (мультиплексора) между сетевым протоколом и многочисленными службами прикладного уровня или пользовательскими процессами.

Прикладной уровень

Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложениям. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и служб прикладного уровня. Прикладной уровень реализуется

программными системами, построенными в архитектуре клиент-сервер, базирующимися на протоколах нижних уровней. В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и «не интересуются» способами передачи данных по сети. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам типа Telnet, FTP, TFTP, DNS, SNMP сравнительно новых служб таких, например, как протокол передачи гипертекстовой информации HTTP.

Уровень сетевых интерфейсов

Идеологическим отличием архитектуры стека TCP/IP от многоуровневой организации других стеков является интерпретация функций самого нижнего уровня - *уровня сетевых интерфейсов.* Протоколы этого уровня должны обеспечивать интеграцию в составную сеть других сетей, причем задача ставится так: сеть TCP/IP должна иметь средства включения в себя любой другой сети, какую бы внутреннюю технологию передачи данных эта сеть не использовала. Отсюда следует, что этот уровень нельзя определить раз и навсегда. Для каждой технологии, включаемой в составную сеть подсети, должны быть разработаны собственные интерфейсные средства. К таким интерфейсным средствам относятся протоколы инкапсуляции IP-пакетов уровня межсетевого взаимодействия в кадры локальных технологий. Например, документ RFC 1042 определяет способы инкапсуляции IP-пакетов в кадры технологий IEEE 802. Для этих целей должен использоваться заголовок LLC/ SNAP, причем в поле Type заголовка SNAP должен быть указан код 0x0800. Только для протокола Ethernet в RFC 1042 сделано исключение - помимо заголовка LLC/ SNAP разрешается использовать кадр Ethernet DIX, не имеющий заголовка LLC, зато имеющий поле Type. В сетях Ethernet предпочтительным является инкапсуляция IP-пакета в кадр Ethernet DIX.

Уровень сетевых интерфейсов в протоколах TCP/IP не регламентируется, но он поддерживает все популярные стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений «точка-точка» SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP за счет разработки соответствующего RFC, определяющего метод инкапсуляции IP-пакетов в ее кадры (спецификация RFC 1577, определяющая работу IP через сети ATM, появилась в 1994 году вскоре после принятия основных стандартов этой технологии).

38. Цифровые абонентские линии

Цифровые выделенные линии образуются путем постоянной коммутации в первичных сетях, построенных на базе коммутационной аппаратуры, работающей на принципах разделения канала во времени - TDM, описанного в главе 2. Существуют два поколения технологий цифровых первичных сетей - технология плезиохронной («плезио» означает «почти», то есть почти синхронной) цифровой иерархии (Plesiochronic Digital Hierarchy, PDH) и более поздняя технология - синхронная цифровая иерархия (Synchronous Digital Hierarchy, SDH). В Америке технологии SDH соответствует стандарт SONET.

Технология плезиохронной цифровой иерархии PDH

Цифровая аппаратура мультиплексирования и коммутации была разработана в конце 60-х годов компанией AT&T для решения проблемы связи крупных коммутаторов телефонных сетей между собой. Каналы с частотным уплотнением, применяемые до этого на участках АТС-АТС, исчерпали свои возможности по организации высокоскоростной многоканальной связи по одному кабелю. В технологии FDM для одновременной передачи данных 12 или 60 абонентских каналов использовалась витая пара, а для повышения скорости связи приходилось прокладывать кабели с большим количеством пар проводов или более дорогие коаксиальные кабели. Кроме того, метод частотного уплотнения высоко чувствителен

к различного рода помехам, которые всегда присутствуют в территориальных кабелях, да и высокочастотная несущая речи сама создает помехи в приемной аппаратуре, будучи плохо отфильтрована.

Для решения этой задачи была разработана аппаратура T1, которая позволяла в цифровом виде мультиплексировать, передавать и коммутировать (на постоянной основе) данные 24 абонентов. Так как абоненты по-прежнему пользовались обычными телефонными аппаратами, то есть передача голоса шла в аналоговой форме, то мультиплексоры T1 сами осуществляли оцифровывание голоса с частотой 8000 Гц и кодировали голос с помощью импульсно-кодовой модуляции (Pulse Code Modulation, PCM). В результате каждый абонентский канал образовывал цифровой поток данных 64 Кбит/с. Для соединения магистральных АТС каналы T1 представляли собой слишком слабые средства мультиплексирования, поэтому в технологии была реализована идея образования каналов с *иерархией скоростей*. Четыре канала типа T1 объединяются в канал следующего уровня цифровой иерархии - T2, передающий данные со скоростью 6,312 Мбит/с, а семь каналов T2 дают при объединении канал T3, передающий данные со скоростью 44,736 Мбит/с. Аппаратура T1, T2 и T3 может взаимодействовать между собой, образуя иерархическую сеть с магистральными и периферийными каналами трех уровней скоростей.

С середины 70-х годов выделенные каналы, построенные на аппаратуре T1, стали сдаваться телефонными компаниями в аренду на коммерческих условиях, перестав быть внутренней технологией этих компаний. Сети T1, а также более скоростные сети T2 и T3 позволяют передавать не только голос, но и любые данные, представленные в цифровой форме, - компьютерные данные, телевизионное изображение, факсы и т. п.

Технология цифровой иерархии была позже стандартизована CCITT. При этом в нее были внесены некоторые изменения, что привело к несовместимости американской и международной версий цифровых сетей. Американская версия распространена сегодня кроме США также в Канаде и Японии (с некоторыми различиями), а в Европе применяется международный стандарт. Аналогом каналов T в международном стандарте являются каналы типа El, E2 и E3 с другими скоростями - соответственно 2,048 Мбит/с, 8,488 Мбит/с и 34,368 Мбит/с. Американский вариант технологии также был стандартизован ANSI.

Несмотря на различия американской и международных версий технологии цифровой иерархии, для обозначения иерархии скоростей принято использовать одни и те же обозначения - DSn (Digital Signal n). В табл. 6.2 приводятся значения для всех введенных стандартами уровней скоростей обеих технологий.

Таблица 6.2. Иерархия цифровых скоростей

	Америка			CCITT (Европа)		
Обозначение скорости	Количество голосовых каналов	Количество каналов предыдущего уровня	Скорость, Мбит/с	Количество голосовых каналов	Количество каналов предыдущего уровня	Скорость, Мбит/с
DS-0	1	1	64 Кбит/с	1	1	64 Кбит/с
DS-1	24	24	1,544	30	30	2,048
DS-2	96	4	6,312	120	4	8,488
DS-3	672	7	44,736	480	4	34,368
DS-4	4032	6	274,176	1920	4	139,264

На практике в основном используются каналы T1/E1 и T3/E3.

Мультиплексор Т1 обеспечивает передачу данных 24-х абонентов со скоростью 1,544 Мбит/с в кадре, имеющем достаточно простой формат. В этом кадре последовательно передается по одному байту каждого абонента, а после 24-х байт вставляется один бит синхронизации. Первоначально устройства Т1 (которые дали имя также и всей технологии, работающей на скорости 1,544 Мбит/с) работали только на внутренних тактовых генераторах, и каждый кадр с помощью битов синхронизации мог передаваться асинхронно. Аппаратура Т1, а также более скоростная аппаратура Т2 и Т3 за долгие годы существования претерпела значительные изменения. Сегодня мультиплексоры и коммутаторы первичной сети работают на централизованной тактовой частоте, распределяемой из одной точки всей сети. Однако принцип формирования кадра остался, поэтому биты синхронизации в кадре по-прежнему присутствуют. Суммарная скорость пользовательских каналов составляет 24 х 64 = 1,536 Мбит/с, а еще 8 Кбит/с добавляют биты синхронизации.

В аппаратуре Т1 назначение восьмого бита каждого байта в кадре разное и зависит от типа передаваемых данных и поколения аппаратуры.

При передаче голоса в сетях Т1 все 24 канала являются абонентскими, поэтому управляющая и контрольная информация передается восьмым (наименее значащим) битом замеров голоса. В ранних версиях сетей Т1 служебным был 8-й бит каждого байта кадра, поэтому реальная скорость передачи пользовательских данных составляла 56 Кбит/с (обычно восьмой бит отводился под такие служебные данные, как номер вызываемого телефонного абонента, сигнал занятости линии, сигнал снятия трубки и т. п.). Затем технология была улучшена и для служебных целей стали использовать только каждый шестой кадр. Таким образом, в пяти кадрах из шести пользовательские данные представлены всеми восемью битами, а в шестом - только семью.

При передаче компьютерных данных канал Т1 предоставляет для пользовательских данных только 23 канала, а 24-й канал отводится для служебных целей, в основном - для восстановления искаженных кадров. Для одновременной передачи как голосовых, так и компьютерных данных используются все 24 канала, причем компьютерные данные передаются со скоростью 56 Кбит/с. Техника использования восьмого бита для служебных целей получила название «кражи бита» (bit robbing).

При мультиплексирования 4-х каналов Т1 в один канал Т2 между кадрами DS-1 по-прежнему используется один бит синхронизации, а кадры DS-2 (которые состоят из 4-х последовательных кадров DS-1) разделяются 12 служебными битами, которые предназначены не только для разделения кадров, но и для их синхронизации. Соответственно, кадры DS-3 состоят из 7 кадров DS-2, разделенных служебными битами.

Международная версия этой технологии описана в стандартах G.700-G.706. Она более логична, так как не использует схему «кражи бита». Кроме того, она основана на постоянном коэффициенте кратности скорости 4 при переходе к следующему уровню иерархии. Вместо восьмого бита в канале Е1 на служебные цели отводятся 2 байта из 32. Для голосовых каналов или каналов данных остается 30 каналов со скоростью передачи 64 Кбит/с каждый.

Пользователь может арендовать несколько каналов 64 Кбит/с (56 Кбит/с) в канале Т1/Е1. Такой канал называется «дробным» (fractional) каналом Т1/Е1. В этом случае пользователю отводится несколько тайм - слотов работы мультиплексора.

Физический уровень технологии PDH поддерживает различные виды кабелей: витую пару, коаксиальный кабель и волоконно-оптический кабель. Основным вариантом абонентского доступа к каналам Т1/Е1 является кабель из двух витых пар с разъемами RJ-48. Две пары требуются для организации дуплексного режима передачи данных со скоростью 1,544/2,048 Мбит/с. Для представления сигналов используется: в каналах Т1 биполярный потенциальный код B8ZS, в каналах El-биполярный потенциальный код HDB3. Для усиления сигнала на линиях Т1 через каждые 1800 м (одна миля) устанавливаются регенераторы и аппаратура контроля линии.

Коаксиальный кабель благодаря своей широкой полосе пропускания поддерживает канал Т2/Е2 или 4 канала Т1/Е1. Для работы каналов Т3/Е3 обычно используется либо коаксиальный кабель, либо волоконно-оптический кабель, либо каналы СВЧ.

Физический уровень международного варианта технологии определяется стандартом G.703, названием которого обозначается тип интерфейса маршрутизатора или моста, подключаемого к каналу Е1. Американский вариант интерфейса носит название Т1.

Как американский, так и международный варианты технологии PDH обладают несколькими недостатками.

Одним из основных недостатков является сложность операций мультиплексирования и демультиплексирования пользовательских данных.Сам термин «плезиохронный», используемый для этой технологии, говорит о причине такого явления - отсутствии полной синхронности потоков данных при объединении низкоскоростных каналов в более высокоскоростные. Изначально асинхронный подход к передаче кадров породил вставку бита или нескольких бит синхронизации между кадрами. В результате для извлечения пользовательских данных из объединенного канала необходимо полностью демультиплексировать кадры этого объединенного канала. Например, если требуется получить данные одного абонентского канала 64 Кбит/с из кадров канала Т3, необходимо произвести демультиплексирование этих кадров до уровня кадров Т2, затем - до уровня кадров Т1, а затем демультиплексировать и сами кадры Т1. Для преодоления этого недостатка в сетях PDH реализуют некоторые дополнительные приемы, уменьшающие количество операций демультиплексирования при извлечения пользовательских данных из высокоскоростных каналов. Например, одним из таких приемов является «обратная доставка» (back hauling). Пусть коммутатор 1 канала Т3 принимает поток данных, состоящий из 672 пользовательских каналов, при этом он должен передать данные одного из этих каналов пользователю, подключенному к низкоскоростному выходу коммутатора, а весь остальной поток данных направить транзитом через другие коммутаторы в некоторый конечный демультиплексор 2, где поток Т3 полностью демультиплексируется на каналы 64 Кбит/с. Для экономии коммутатор 1 не выполняет операцию демультиплексирования своего потока, а получает данные своего пользователя только при их «обратном проходе», когда конечный демультиплексор выполнит операцию разбора кадров и вернет данные одного из каналов коммутатору 1. Естественно, такие сложные взаимоотношения коммутаторов усложняют работу сети, требуют ее тонкого конфигурирования, что ведет к большому объему ручной работы и ошибкам.

Другим существенным недостатком технологии PDH является отсутствие развитых встроенных процедур контроля и управления сетью. Служебные биты дают мало информации о состоянии канала, не позволяют его конфигурировать и т. п. Нет в технологии и процедур поддержки отказоустойчивости, которые очень полезны для первичных сетей, на основе которых строятся ответственные междугородные и международные сети. В современных сетях управлению уделяется большое внимание, причем считается, что управляющие процедуры желательно встраивать в основной протокол передачи данных сети.

Третий недостаток состоит в слишком низких по современным понятиям скоростях иерархии PDH. Волоконно-оптические кабели позволяют передавать данные со скоростями в несколько гигабит в секунду по одному волокну, что обеспечивает консолидацию в одном кабеле десятков тысяч пользовательских каналов, но это свойство технология PDH не реализует - ее иерархия скоростей заканчивается уровнем 139 Мбит/с.

Все эти недостатки устранены в новой технологии первичных цифровых сетей, получившей название *синхронной цифровой иерархии - Synchronous DigitalHierarchy, SDH.*

Технология синхронной цифровой иерархии SONET/SDH

Технология синхронной цифровой иерархии первоначально была разработана компанией Bellcore под названием «Синхронные оптические сети» - Synchronous Optical NETs, SONET. Первый вариант стандарта появился в 1984 году. Затем эта технология была стандартизована комитетом T1 ANSI. Международная стандартизация технологии проходила под эгидой Европейского института телекоммуникационных стандартов (ETSI) и CCITT совместно с ANSI и ведущими телекоммуникационными компаниями Америки, Европы и Японии. Основной целью разработчиков международного стандарта было создание такой технологии, которая позволяла бы передавать трафик всех существующих цифровых каналов (как американских T1 - T3, так и европейских E1 - E3) в рамках высокоскоростной магистральной сети на волоконно-оптических кабелях и обеспечила бы иерархию скоростей, продолжающую иерархию технологии PDH, до скорости в несколько гигабит в секунду.

В результате длительной работы удалось разработать международный стандарт Synchronous Digital Hierarchy, SDH (спецификации G.707-G.709), а также доработать стандарты SONET таким образом, что аппаратура и стеки SDH и SONET стали совместимыми и могут мультиплексировать входные потоки практически любого стандарта PDH - как американского, так и европейского. В терминологии и начальной скорости технологии SDH и SONET остались расхождения, но это не мешает совместимости аппаратуре разных производителей, а технология SONET/ SDH фактически стала считаться единой технологией. В России применяются стандарты и адаптированная терминология SDH.

Иерархия скоростей при обмене данными между аппаратурой SONET/SDH, которую поддерживает технология SONET/SDH, представлена в табл. 6.3.

Таблица 6.3. Скорости технологии SONET/SDH

SDH	SONET	Скорость
—	STS-1, OC-1	51,840 Мбит/с
STM-1	STS-3, OC-3	155,520 Мбит/с
STM-3	STS-9, OC-9	466,560 Мбит/с
STM-4	STS-12, OC-12	622,080 Мбит/с
STM-6	STS-18, OC-18	933,120 Мбит/с
STM-8	STS-24, OC-24	1,244 Гбит/с
STM-12	STS-36, OC-36	1,866 Гбит/с
STM-16	STS-48, OC-48	2,488 Гбит/с

В стандарте SDH все уровни скоростей (и, соответственно, форматы кадров для этих уровней) имеют общее название: STM-n - Synchronous Transport Module level n. В технологии SONET существуют два обозначения для уровней скоростей: STS-n - Synchronous Transport Signal level n, употребляемое при передаче данных электрическим сигналом, и OC-n - Optical Carrier level n, употребляемое при передаче данных световым лучом по волоконно-оптическому кабелю. Форматы кадров STS и OC идентичны.

Как видно из таблицы, стандарт SONET начинается со скорости 51,84 Мбит/с, а стандарт SDH - со скорости 155,52 Мбит/с, равной утроенной начальной скорости SONET. Международный стандарт определил начальную скорость иерархии в 155,52 Мбит/с, чтобы сохранялась стройность и преемственность технологии SDH с технологией PDH - в этом случае канал SDH может передавать данные уровня DS-4, скорость которых равна 139,264 Мбит/с. Любая скорость технологии SONET/ SDH кратна скорости STS-1. Некоторая избыточность скорости 155,52 Мбит/с для передачи данных уровня DS-4 объясняется большими накладными расходами на служебные заголовки кадров SONET/SDH.

Кадры данных технологий SONET и SDH, называемые также циклами, по форматам совпадают, естественно начиная с общего уровня STS-3/STM-1. Эти кадры обладают весьма большой избыточностью, так как передают большое количество служебной информации, которая нужна для:

- обеспечения гибкой схемы мультиплексирования потоков данных разных скоростей, позволяющих вставлять (add) и извлекать (drop) пользовательскую информацию любого уровня скорости, не демультиплексируя весь поток;
- обеспечения отказоустойчивости сети;
- поддержки операций контроля и управления на уровне протокола сети;
- синхронизации кадров в случае небольшого отклонения частот двух сопрягаемых сетей.

Стек протоколов и основные структурные элементы сети SONET/SDH показаны на рис. 6.7.

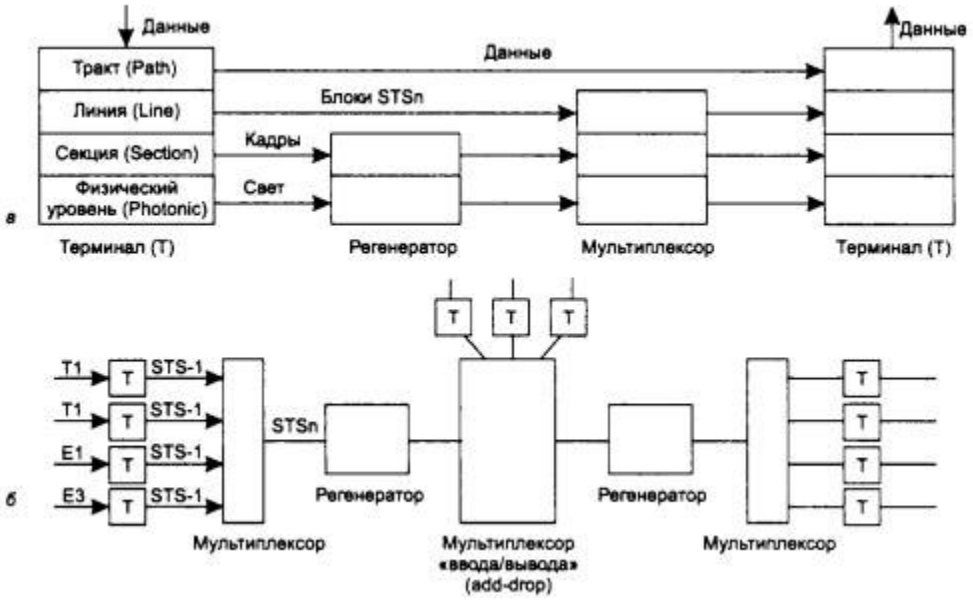


Рис. 6.7. Стек протоколов и структура сети SONET/SDH

Ниже перечислены устройства, которые могут входить в сеть технологии SONET/ SDH.

- *Терминальные устройства (Terminal, T),* называемые также сервисными адаптерами (Service Adapter, SA), принимают пользовательские данные от низкоскоростных каналов технологии PDH (типа T1/E1 или T3/E3) и преобразуют их в кадры STS-n. (Далее аббревиатура STS-n используется как общее обозначение для кадров SONET/SDH.)
- *Мультиплексоры (Muliplexers)* принимают данные от терминальных устройств и мультиплексируют потоки кадров разных скоростей STS-n в кадры более высокой иерархии STS-m.
- *Мультиплексоры «ввода-вывода» (Add-Drop Multiplexers)* могут принимать и передавать транзитом поток определенной скорости STS-n, вставляя или удаляя «на ходу», без полного демультиплексирования, пользовательские данные, принимаемые с низкоскоростных входов.
- *Цифровые кросс-коннекторы (Digital Cross-Connect, DCC)*, называемые также аппаратурой оперативного переключения (АОП), предназначены для мультиплексирования и постоянной коммутации высокоскоростных потоков STS-n различного уровня между собой (на рис. 6.7 не показаны). Кросс-коннектор представляет собой разновидность мультиплексора, основное назначение которого - коммутация высокоскоростных потоков данных, возможно, разной скорости. Кросс-коннекторы образуют магистраль сети SONET/SDH.
- *Регенераторы сигналов*, используемые для восстановления мощности и формы сигналов, прошедших значительное расстояние по кабелю. На практике иногда сложно провести четкую грань между описанными устройствами, так как многие производители выпускают многофункциональные устройства, которые включают терминальные модули, модули «ввода-вывода», а также модули кросс-коннекторов.

Стек протоколов состоит из протоколов 4-х уровней.

- *Физический уровень,* названный в стандарте *фотонным (photonic)*, имеет дело с кодированием бит информации с помощью модуляции света. Для кодирования сигнала применяется метод NRZ (благодаря внешней тактовой частоте его плохие самосинхронизирующие свойства недостатком не являются).
- *Уровень секции (section)* поддерживает физическую целостность сети. Секцией в технологии называется каждый непрерывный отрезок волоконно-оптического кабеля, который соединяет пару устройств SONET/SDH между собой, например мультиплексор и регенератор. Протокол секции имеет дело с кадрами и на основе служебной информации кадра может проводить тестирование секции и поддерживать операции административного контроля. В заголовке протокола секции имеются байты, образующие звуковой канал 64 Кбит/с, а также канал передачи данных управления сетью со скоростью 192 Кбит/с. Заголовок секции всегда начинается с двух байт 11110110 00101000, которые являются флагами начала кадра. Следующий байт определяет уровень кадра: STS-1, STS-2 и т. д. За каждым типом кадра закреплен определенный идентификатор.
- *Уровень линии (line)* отвечает за передачу данных между двумя мультиплексорами сети. Протокол этого уровня работает с кадрами разных уровней STS-n для выполнения различных операций мультиплексирования и демультиплексирования, а также вставки и удаления пользовательских данных. Таким образом, линией называется поток кадров одного уровня между двумя мультиплексорами. Протокол линии также ответственен за проведения операций реконфигурирования линии в случае отказа какого-либо ее элемента - оптического волокна, порта или соседнего мультиплексора.
- *Уровень тракта (path - путь)* отвечает за доставку данных между двумя конечными пользователями сети. Тракт (путь) - это составное виртуальное соединение между пользователями. Протокол тракта должен принять данные, поступающие в пользовательском формате, например формате T1, и преобразовать их в синхронные кадры STS-n/STM-m.

Как видно из рис. 6.7, регенераторы работают только с протоколами двух нижних уровней, отвечая за качество сигнала и поддержания операций тестирования и управления сетью. Мультиплексоры работают с протоколами трех нижних уровней, выполняя, кроме функций регенерации сигнала и реконфигурации секций, функцию мультиплексирования кадров STS-n разных уровней. Кросс-коннектор представляет собой пример мультиплексора, который поддерживает протоколы трех уровней. И наконец, функции всех четырех уровней выполняют терминалы, а также мультиплексоры «ввода-вывода», то есть устройства, работающие с пользовательскими потоками данных.

Формат кадра STS-1 представлен на рис. 6.8. Кадры технологии SONET/SDH принято представлять в виде матрицы, состоящей из n строк и m столбцов. Такое представление хорошо отражает структуру кадра со своего рода подкадрами, называемыми виртуальными контейнерами (Virtual Container, VC - термин SDH) или виртуальными притоками (Virtual Tributaries, VT - термин SONET). Виртуальные контейнеры - это подкадры, которые переносят потоки данных, скорости которых ниже, чем начальная скорость технологии SONET/SDH в 51,84 Мбит/с (например, поток данных T1 со скоростью 1,544 Мбит/с).

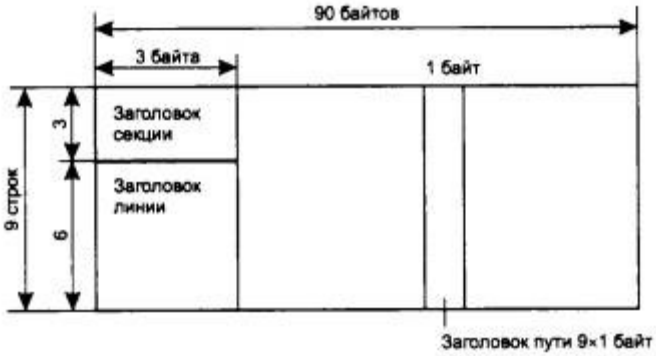


Рис. 6.8. Формат кадра STS-1

Кадр STS-1 состоит из 9 строк и 90 столбцов, то есть из 810 байт данных. Между устройствами сети кадр передается последовательно по байтам - сначала первая строка слева направо, затем вторая и т. д. Первые 3 байта каждой строки представляют собой служебные заголовки. Первые 3 строки представляют собой заголовок из 9 байт протокола уровня секции и содержат данные, необходимые для контроля и реконфигурации секции. Остальные 6 строк составляют заголовок протокола линии, который используется для реконфигурации, контроля и управления линией. Устройства сети SONET/SDH, которые работают с кадрами, имеют достаточный буфер для размещения в нем всех байт кадра, протекающих синхронно через устройство, поэтому устройство для анализа информации на некоторое время имеет полный доступ ко всем частям кадра. Таким образом, размещение служебной информации в несмежных байтах не представляет сложности для обработки кадра.

Еще один столбец представляет собой заголовок протокола пути. Он используется для указания местоположения виртуальных контейнеров внутри кадра, если кадр переносит низкоскоростные данные пользовательских каналов типа T1/E1. Местоположение виртуальных контейнеров задается не жестко, а с помощью системы *указателей (pointers)*.

Концепция указателей является ключевой в технологии SONET/SDH. Указатель призван обеспечить синхронную передачу байт кадров с асинхронным характером вставляемых и удаляемых пользовательских данных.

Указатели используются на разных уровнях. Рассмотрим, как с помощью указателя выполняется выделение поля данных кадра из синхронного потока байт. Несмотря на питание всех устройств сети SONET/SDH тактовой частотой синхронизации из одного центрального источника, синхронизация между различными сетями может незначительно нарушаться. Для компенсации этого эффекта началу поля данных кадра (называемого в стандарте SPE - Synchronous Payload Environment) разрешается смещаться относительно начала кадра произвольным образом. Реальное начало поля SPE задается указателем HI, размещенным в заголовке протокола линии. Каждый узел, поддерживающий протокол линии, обязан следить за частотой поступающих данных и компенсировать ее несовпадение с собственной частотой за счет вставки или удаления одного байта из служебного заголовка. Затем узел должен нарастить или уменьшить значения указателя первого байта поля данных CPE относительно начала кадра STS-1. В результате поле данных может размещаться в двух последовательных кадрах, как это показано на рис. 6.9.

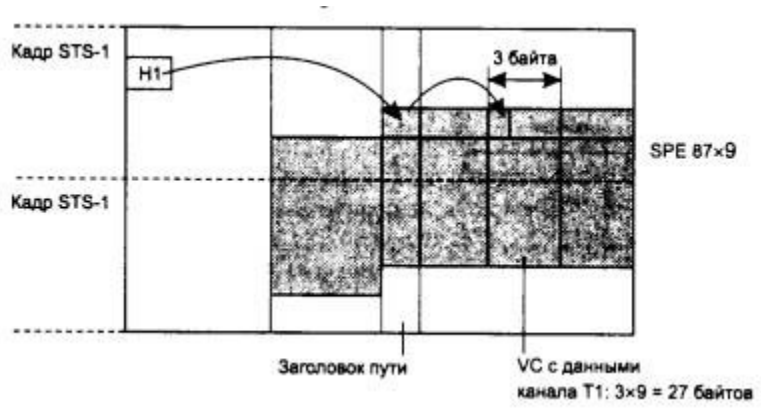


Рис. 6.9. Использование указателей для поиска данных в кадре

Тот же прием применяется для вставки или удаления пользовательских данных в потоке кадров STS-n. Пользовательские данные каналов типа T1/E1 или T3/E3 асинхронны по отношению к потоку байтов кадра STS-n. Мультиплексор формирует виртуальный контейнер и, пользуясь указателем HI, находит начало очередного поля данных. Затем мультиплексор анализирует заголовок пути и находит в нем указатель H4, который описывает структуру содержащихся в кадре виртуальных контейнеров. Обнаружив свободный виртуальный контейнер нужного формата, например для 24 байт канала T1, он вставляет эти байты в нужное место поля данных кадра STS-1. Аналогично производится поиск начала данных этого канала при выполнении операции удаления пользовательских данных.

Таким образом, кадры STS-n всегда образуют синхронный поток байтов, но с помощью изменения значения соответствующего указателя можно вставить и извлечь из этого потока байты низкоскоростного канала, не выполняя полного демультиплексирования высокоскоростного канала.

Виртуальные контейнеры также содержат дополнительную служебную информацию по отношению к данным пользовательского канала, который они переносят. Поэтому виртуальный контейнер для переноса данных канала T1 требует скорости передачи данных не 1,544 Мбит/с, а 1,728 Мбит/с.

В технологии SONET/SDH существует гибкая, но достаточно сложная схема использования поля данных кадров STS-n. Сложность этой схемы в том, что нужно «уложить» в кадр наиболее рациональным способом мозаику из виртуальных контейнеров разного уровня. Поэтому в технологии SONET/SDH стандартизовано шесть типов виртуальных контейнеров, которые хорошо сочетаются друг с другом при образовании кадра STS-n. Существует ряд правил, по которым контейнеры каждого вида могут образовывать группы контейнеров, а также входить в состав контейнеров более высокого уровня.

Отказоустойчивость сети SONET/SDH встроена в ее основные протоколы. Этот механизм называется автоматическим защитным переключением - Automatic Protection Switching, APS. Существуют два способа его работы. В первом способе защита осуществляется по схеме 1:1. Для каждого рабочего волокна (и обслуживающего его порта) назначается резервное волокно. Во втором способе, называемом 1:n, для защиты n волокон назначается только одно защитное волокно.

В схеме защиты 1:1 данные передаются как по рабочему, так и по резервному волокну. При выявлении ошибок принимающий мультиплексор сообщает передающему, какое волокно должно быть рабочим. Обычно при защите 1:1 используется схема двух колец, похожая на двойные кольца FDDI (рис. 6.10), но только с одновременной передачей данных в противоположных направлениях. При обрыве кабеля между двумя мультиплексорами происходит сворачивание колец, и, как и в сетях FDDI, из двух колец образуется одно рабочее.

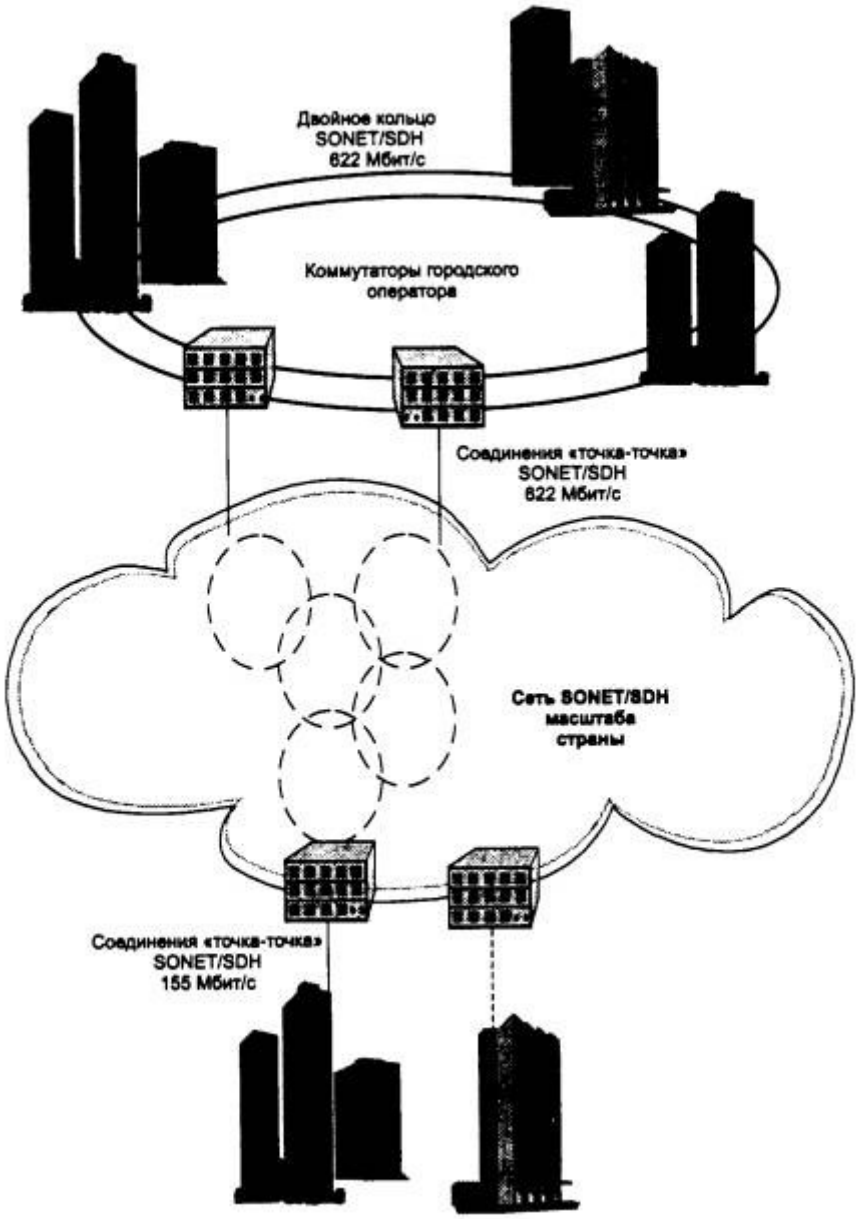


Рис. 6.10. Использование двойных колец для обеспечения отказоустойчивости сети SONET/SDH

Применение схемы резервирования 1:1 не обязательно требует кольцевого соединения мультиплексоров, можно применять эту схему и при радиальном подключении устройств, но кольцевые структуры решают проблемы отказоустойчивости эффективнее - если в сети нет колец, радиальная схема не сможет ничего сделать при обрыве кабеля между устройствами.

Управление, конфигурирование и администрирование сети SONET/SDH также встроено в протоколы. Служебная информация протокола позволяет централизованно и дистанционно конфигурировать пути между конечными пользователями сети, изменять режим коммутации потоков в кросс-коннекторах, а также собирать подробную статистику о работе сети. Существуют мощные системы управления сетями SDH, позволяющие прокладывать новые каналы простым перемещением мыши по графической схеме сети.

41. Источники сообщений. Три процедуры преобразования аналог–цифра.

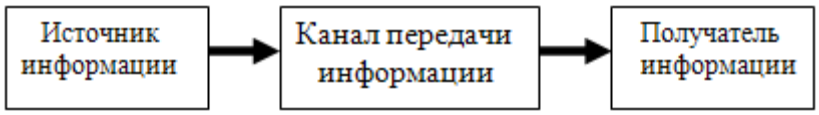
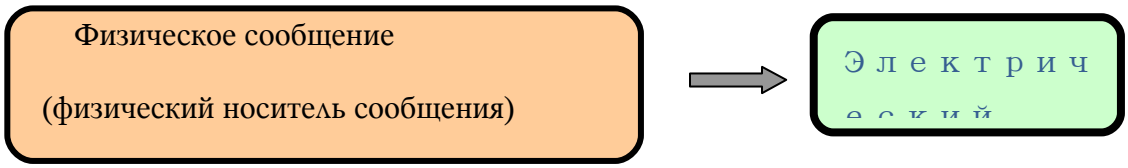


Рис.2 Метаструктура СПИ

Источник информации (ИИ):



Сигналы: информационные (управляющие), переносчики.

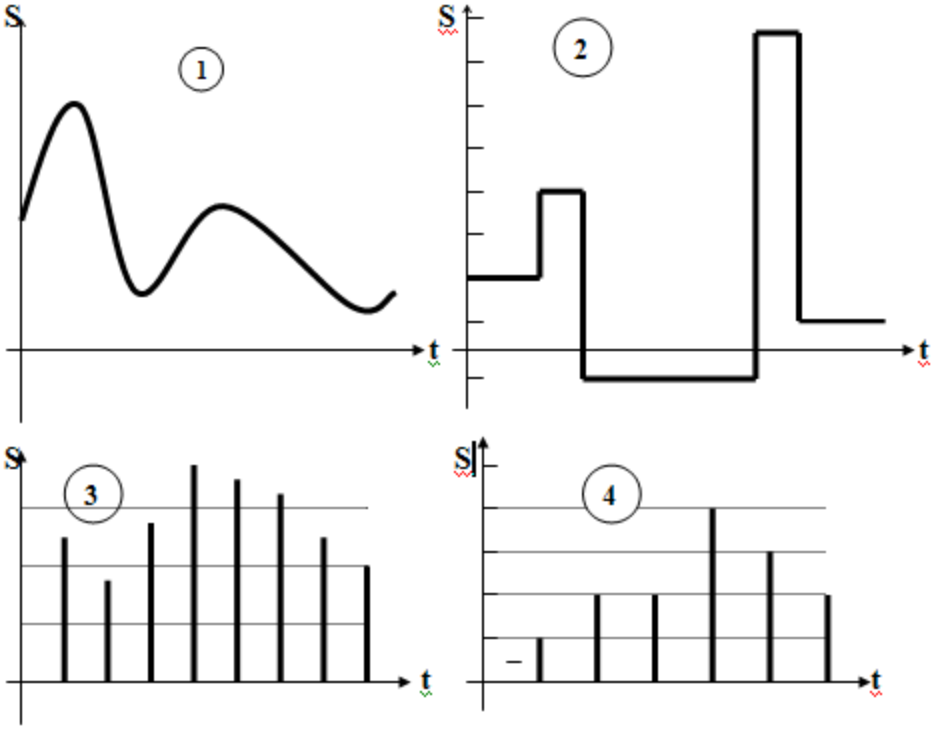


Рис. 3 Модели сигналов.

1. непрерывный по времени и по уровню;
2. дискретный по уровню и непрерывный по времени;
3. дискретный по времени и непрерывный по уровню;
4. дискретный по времени и по уровню.

Кодирование источника.

Источники: терминалы (ПК), ЭВМ (хост, сервер). автоматические датчики.

Для представления символьной информации в ЭВМ общего назначения применяют ***двоичный код обработки информации*** **– ДКОИ.** Кодировка символов осуществляется с помощью таблицы: в первой строке и первом столбце таблицы указаны значения старшей и младшей тетрады байта соответственно.

В мини- и микро ЭВМ для представления символьной информации часто используется специальный ***код обмена информацией*****: КОИ-7.**

В том и другом случае для представления символов используется один байт. В КОИ-7 используется для кодирования только 7 разрядов байта. Левый разряд каждого байта в КОИ-7 равен 0.

Во многих микропроцессорных системах и персональных ЭВМ для представления алфавитно-цифровых символов используется код **ASCII** (***American Standart Code for Information Interchange*** – американский код обмена информацией), расширенный путем добавления букв русского алфавита. Для представления каждого символа отводится один байт.

Все виды представления символьной информации отличаются только кодировкой символов.

При кодировании аналоговых сигналов, снимаемых с автоматических датчиков, кодирование источника осуществляется с использованием трех процедур: дискретизации, квантования, кодирования.

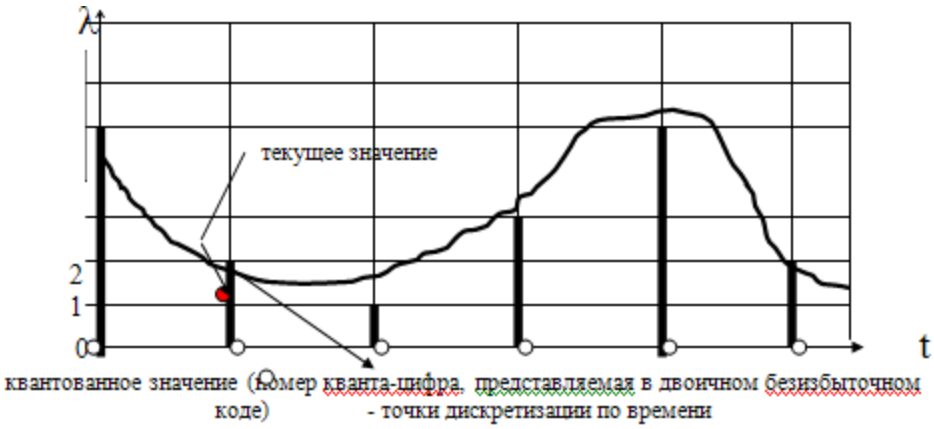


Рис. 4. Дискретизация, квантование, кодирование

Дискретизация, квантование, кодирование ⟹ «цифровой сигнал»
⇒ ИКМ – импульсно - кодовая модуляция.

42. Каналы связи (КС). Функциональная структура КС. Физическая среда.

<u>Физические характеристики сигналов и каналов:</u>

Тс – временная длительность;

Fс – ширина спектра;

Hc = log(Pc/ Pш) – превышение (Pc –средняя мощность сигнала, Pш - средняя (эффективная) мощность помехи);

Vc = Tc·FcHc – объем сигнала;

Tc Fc – широкополосность сигнала; Tc· Fc>>1 – широкополосный сигнал.

Vк = Tк·FкHк – емкость канала;

Vк ≥ Vc – условие (идеальное) неискаженной передачи сигнала.

<u>Понятие канала связи</u>

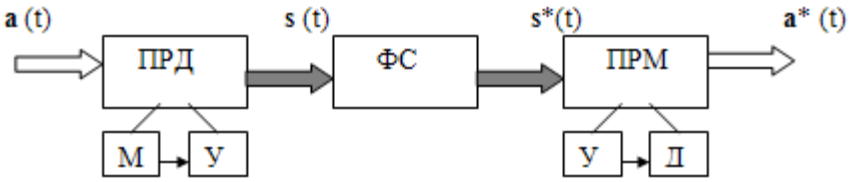


Рис.5. Функциональная структура канала связи

a (t) – управляющий(информационный) сигнал;

s (t) –промодулированный сигнал – переносчик;

ПРД – передатчик (М – модулятор, У – усилитель);

ПРМ – приемник)Д – демодулятор);

ФС – физическая среда передачи сигналов данных.

Физическая среда передачи сигналов данных определяет линию связи и может представлять собой кабель, то есть набпр проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу и космическое пространство, через которые распространяются электромагнитные волны (радиосигналы).

Различают линии связи:

- проводные (воздушные);
- кабельные (медные и волоконно – оптические);
- радио линии наземной и спутниковой связи.

Каждая среда характеризуется частотным диапазоном, в котором наиболее благоприятны условия для передачи сигналов.

Проводные (воздушные) линии связи представляют собой провода без изолирующих и экранирующих оплеток, проложенные между столбаи и висящие в воздухе. Скоростные качества и помехозащищенность низкие. Частотный диапазон 10 –150 кГц, до 500 кГц у ЛЭП.

Кабельные линии представляют собой довольно сложную конструкцию. Кабель состоит из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической, возможно и климатической. Может быть оснащен разъемами. В компьютерных сетях для передачи данных используются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой и волоконно-оптические кабели.

Скрученная пара проводой называется *витой парой (twsted pair)* Витая пара существует в экранированном варианте (Shielded T*wsted Pair, STP)* и неэкранированном (Unshielded T*wsted Pair, UTP)*, когда изоляционная обертка отсутствует. Каждая витая пара имеет свою граничную частоту. В локальных сетях это 10-100 мГц. Каждая среда вносит затухание в передаваемый сигнал. Витая пара отличается высокой степенью затухания и высокой чувствительностью к высокочастотным помехам. Из за этого дальность передачи по витой паре не превышает 100 метров.

Коаксиальный кабель (coaxial) имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилыслоем изодяции (Рис.6).

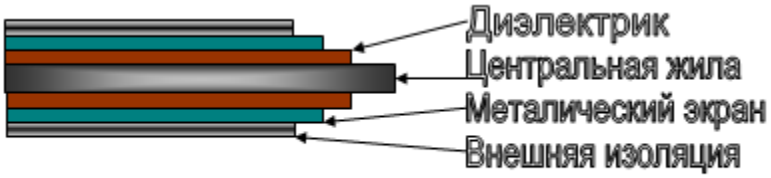
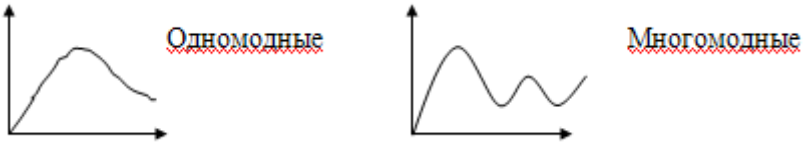


Рис.6. Конструкция коаксиального кабеля

Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения – для локальных сетей, глобальных сетей, для кабельного телевидения. Расстояние между передающими устройствами до двух километров. Граничная частота до 100 мГц.Обычные скорости ПД - 2.5 ÷ 100 мбит/сек.

Волоконно-оптоволоконный кабель состоит из тонких (5-60 микрон) волокон, по которым распространяются световые сигналы. Частотный диапазон. 1000-10000 гГц, скорости ПД 2 и более гбит/сек.

Существует два типа источников света: одномодовые и многомодовые.



При одномодном источнике расстояние до 100 км, при многомодовом около 4 км. Это естественно вытекает из физики явления: одномодовый источник выдает жестко сфокусированный пучок; многомодовый – значительно более рассеянный.

Радиоканалы наземной и спутниковой связи отличаются большим разнообразием как используемым частотным диапазоном, так и дальностью действия. Для радио релейных линий (РРЛ) характерен диапазон 60 мГц-15гГц; для спутниковых каналов – до сотен гГц. Спутниковые каналы и другую радиосвязь используют, когда кабельные линии применить нельзя.

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам. Стандарты определяют характеристики не отдельного кабеля, а полного набора элементов, необходимого для создания кабельного соединения (например, шнура от рабочей станции до розетки, сомой розетки, основного кабеля, жесткого кроссового соединения и шнура до концентратора. (Наиболее употребительные стандарты см. Компьютерные сети. Принципы, технологии, протоколы / В.Г.Олифер, Н.А.Олифер. – СПб: Издательство «Питер», 1999. – 672с.)

43. Классификация КС. Электрические характеристики КС.

ЭЛЕКТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ КАНАЛОВ СВЯЗИ

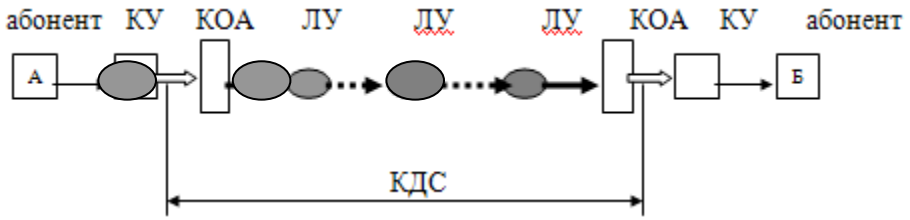


Рис. 7. Структура канала связи

КУ – коммутационный узел;

КОА – каналообразующая аппаратура;

ЛУ – линейный усилитель;

<u>КДС канал дальней связи</u>

Качество КС оценивается электрическими характеристиками:

1). Остаточным затуханием – аост;

2). АЧХ;

3). ФЧХ или ЧХ tгр;

4). АХ (коэффициентом неблинейных искажений);

5). Уровнем помех на выходе канала.

1. Остаточное затухание

Коэффициент распространения сигнала по цепи

$$\gamma = \sqrt{(R + j\omega L)(G + j\omega C)}$$

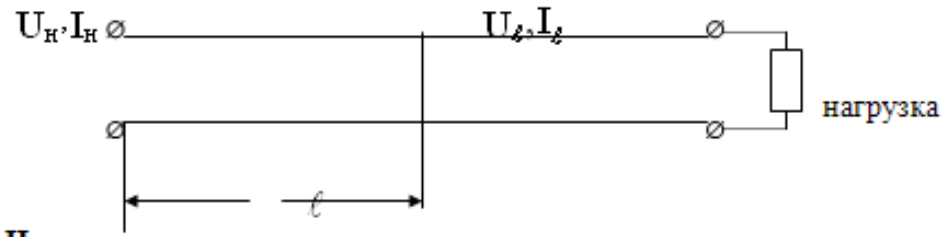


Рис.8. Нагруженная электрическая цепь

<u>При согласованной нагрузке</u>

$$U_\ell = U_н\, e^{-\gamma\ell}; \quad I_\ell = I_н\, e^{-\gamma\ell}; \quad \gamma=\alpha+j\beta;$$

$\alpha\ell$ =a – характеристическое (собственное) затухание цепи;

$\beta\ell$ = b – характеристический фазовый сдвиг цепи;

α и β - километровые затухание и сдвиг.

Дальность есть F(a). Для двухпроводного телефонного канала аост = 0,8 Неп.

$$\ell_{\max} = \frac{0{,}8}{\alpha}$$

Симметричный стальной кабель диаметром 1,2 мм имеет α=41[мНеп / км], из чего следует $\ell_{\max}$ =19,5 км. Поэтому необходимы специальные меры для увеличения дальности.

$$а_{ост} = \sum_i a_i - \sum_j s_j ,$$

где a_i - рабочее затухание i-го участка канала,

s_j - рабочее усиление j-го линейного усилителя.

a_i =(1/2)·ln (Рвх / Р вых); s_j - рабочее усиление j-го ЛУ.

$а_{ост}$ нормируется. Для двухпроводного канала $а_{ост}$ = 0,8 Неп; для четырехпроводного канала – $а_{ост}$ = 0 или $а_{ост}$ = –2 Неп (остаточное усиление).

2.**АЧХ** : аост = φ($F_{[герц]}$)

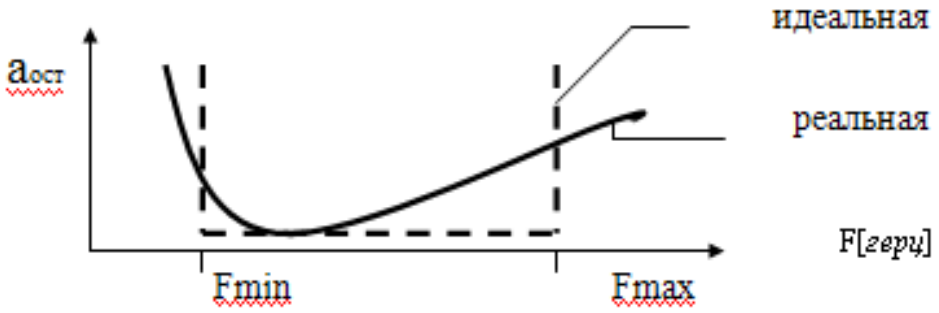


Рис.9. Амплитудно-частотная характеристика КС

На практике вместо АЧХ применяют упрощенные характеристики: полосу пропускания и затухание на основной частоте передаваемого сигнала (частота, гармоника которой имеет наибольшую амплитуду и мощность).

Полоса пропускания – это непрерывный диапазон частот, для которого отношение выходного сигнала ко входному превышает некоторый заранее заданный предел, обычно 0,5. Полоса пропускания зависит от типа линнии связи и от ее протяженности.

Затухание измеряется в неперах (Неп) или в децибелах (дБ):

a=(1/2)ln(Рвх / Рвых) (Неп); a=(1/2)log(Рвх / Рвых) (дБ);

1дБ≈0,115 Нп; 1Нп≈8,69 дБ

3. **ФЧХ** – зависимость от частоты сдвига фазы сигнала на выходе канала относительно фазы сигнала на входе канала.

Практически фазовые сдвиги определяют, пользуясь групповым временем распространения сигнала tгр (время необходимое для пробега по каналу максимума огибающей сигнала). Нормируются отклонения на крайних частотах.

4. **АХ** – это зависимость уровня сигнала на выходе канала от уровня сигнала на входе канала. Оцениваются часто коэффициентом нелинейных искажений:

$$\text{Кни} = \left(\frac{U_{2m}^2 + U_{3m}^2 + \ldots}{U_{1m}^2} \right)^{1/2} \cdot 100\,\%$$

Значение коэффициента нормируется. Например, для телефонного КДС Кни ¿ 1,5/2500 км

5. Уровень помех на выходе канала определяется

- нестабильностью во времени коэффициента передачи канала;

- кратковременные разрывы канала (понижение уровня более, чем на 0,7 Неп);
- скачки уровня в пределах $|0{,}2 \div 0{,}7|$ Неп
- посторонние сигналы (помехи, шум).

Существуют различные модели, описывающие конечные искажения сигналов на выходе канала (модели каналов).

<u>Примеры моделей каналов.</u>

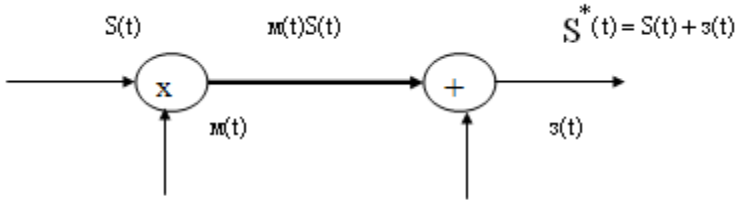


Рис.10. Модель непрерывного канала
м(t) - мультипликативная помеха,
з(t) - аддитивная помеха

Наиболее распространенная модель непрерывного канала - ***гауссов канал***. Модель отображает канал, в котором действует лишь аддитивная флюктуационная помеха (μ(t)=1)

$$S^{¿}(t) = S(t) + \eta(t)$$

Процесс полагается стационарным, т е.

$$S^{¿}(t) = S(t) + \eta$$

и представляет собой гауссовый случайный процесс без постоянной составляющей, чаще всего полагаемый белым шумом в полосе частот КС. Мгновенные значения ***x*** распределены нормально с плотностью

$$w(x) = \frac{1}{\sqrt{2\pi}\,\sigma} e^{-\frac{x^2}{2\sigma^2}}$$

Характеристики огибающей:

Пауза – огибающая помехи (распределение значений по закону Релея)

$$W0(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}$$

Посылка – огибающая сигнал плюс помеха (обобщенный закон Релея)

$$W1(x)=\frac{x}{\sigma^2}e^{-\frac{x^2+A^2}{2\sigma^2}}I_0\left(\frac{x+A}{\sigma^2}\right),$$

где А – амплитуда синусоидального сигнала переносчика логической «1»;

I_0 - функция Бесселя нулевого порядка;

σ^2 - мощность (дисперсия) шума.

Обобщающими характеристиками канала, которые отображают как ограничения на входные сигналы, так и на степень воздействия помехи, являются

- ширина полосы пропускания ΔFk;
- отношение $h_к^2$ =(Pc / Pξ) средней мощности сигнала к средней мощности помехи.

<u>Модели дискретного канала</u>

Модели дискретного канала (ДК) должны адекватно отображать характер преобразования входной битовой последовательности в выходную.

Модель ДК описывает вероятностные характеристики последовательности ошибок на выходе ДК. Удобным отображением ошибки является ***вектор ошибки*** – последовательность двоичных элементов длиной **n**, в которой “единица” стоит на позиции, где произошла ошибка, и “ноль” на позиции, элемент которой принят правильно.

Различают ДК с независимыми и группирующимися ошибками.

Дискретный симметричный канал без памяти является моделью канала с независимыми ошибками. В таком канале вероятность P(n,j) появления какой либо ошибки кратности j есть

$$P(n,j)=C_n^j p^j(1-p)^{n-j}.$$

Вероятность правильного приема n-последовательности

$$Q(n)=P(n,0)=(1-p)^n\approx 1-\mathrm{np}\text{, при (np<<1)}$$

Вероятность появления какой либо ошибки в n-последовательности

$$P(n)=\sum_{j=1}^{n}C_n^j p^j(1-p)^{n-j}=1-Q(n)\approx \mathrm{np}.$$

Примером модели, описывающей группирующиеся в пакет ошибки, является параметрическая модель Пуртова. Модель включает два параметра:

p – вероятность ошибки при приеме двоичного символа;

α, (0 ≤ α ≥ 1) – коэффициент группирования ошибок.

Приближенно модель (верхняя оценка) записывается следующим образом

$$P(\geq j, n) \approx \left(\frac{n}{j}\right)^{1-\alpha} \cdot p, \quad P(j, n) = P(\geq j, n) - P(\geq j+1, n).$$

В реальном канале встречаются все типы ошибок. Чем выше качество канала (меньше значение p), тем большую долю составляют независимые ошибки. Чем больше канал подвержен воздействию импульсных помех, тем ниже его качество, и основную роль играют ошибки, группирующиеся в пакеты.

44. Типы каналов дальней связи: каналы НЧ, широкополосные (уплотненные) каналы

Каналы низкой частоты (НЧ)

Канал, образованный непосредственно по физической цепи называют каналом НЧ. Различают два типа телефонных КДС; двхпроводный и четырехпроводный. Основной способ увеличения дальности – применение промежуточных усилителей.

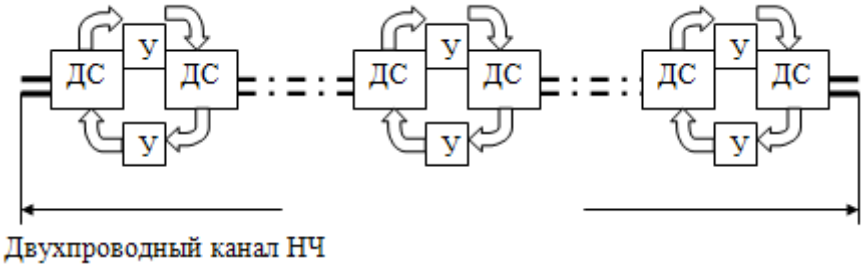


Рис.11. Структура двухпроводного КДС НЧ

ДС – дифференциальная система, У – усилитель

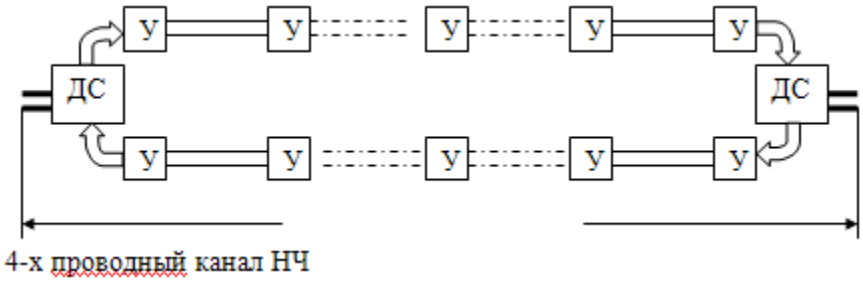


Рис.12. Структура 4-х проводного КДС НЧ

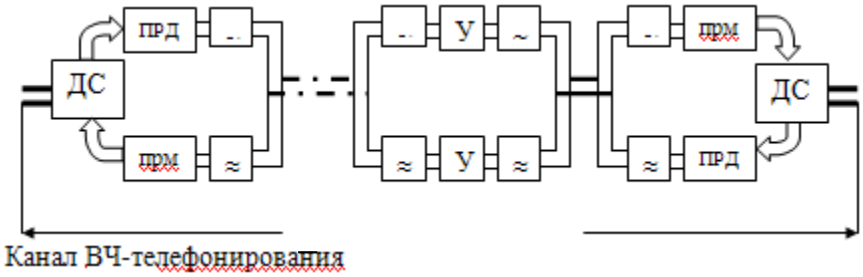


Рис.13. Структура канала ВЧ-телефонирования

ПРД – передатчик; прм-приемник;

- полосовой фильтр нижних частот;
- полосовой фильтр верхних частот

ШИРОКОПОЛОСНЫЙ КАНАЛ с ЧУ (частотным уплотнением)

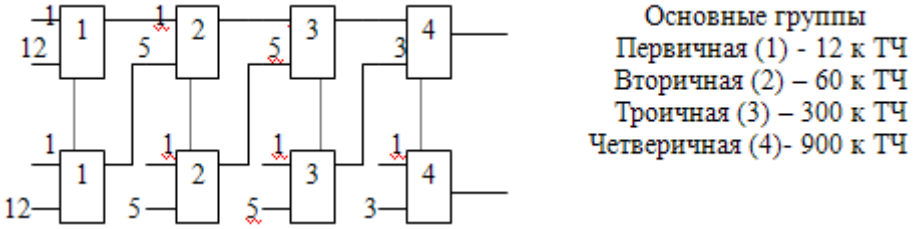


Рис.15. ИЕРАРХИЯ СТАНДАРТНЫХ КАНАЛОВ с ЧУ

Канал для передачи групповых сигналов. Образуется за счет АУ. За основу АУ приняты канал тональных частот (ТЧ) и блок, рассчитанный на уплотнение одного широкополосного канала 12-ю телефонными каналами.

ШИРОКОПОЛОСНЫЙ КАНАЛ с ВУ (временным уплотнением)

Частота дискретизации $F_Д$ = 8 кГц; при ИКМ с n = 8 (разрядность кодового слова) минимальная скорость передачи на один телефонный канал равна

$$C1 = n\ F_Д = 64\ кБод$$

Канал для передачи групповых сигналов образуется за счет АУ. За основу АУ приняты телефонный канал с ИКМ и блок, рассчитанный на уплотнение одного широкополосного канала 30-ю телефонными каналами.

ПГ = 30 инф. Кан. + 2служ кан. (ПГ – первичная группа)

С30 = 32·64 = 2048 кБод;

ВГ – уплотнение во времени 4-х ПГ + 4 служ кан.(для синхронизации циклов ВГ):

С120 = (32·4+4)·64=8448 кБод;

ТГ = 4 ВГ+9 служ.кан.(для синхронизации циклов ТГ):

С480 = 34368 кБод;

ЧГ = 4 ТГ+28служ.кан.(для синхронизации циклов ЧГ):

С1920 = 139264 кБод.

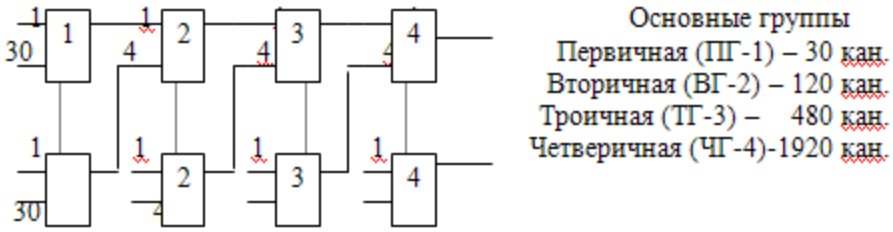


Рис.16. ИЕРАРХИЯ СТАНДАРТНЫХ КАНАЛОВ с ВУ

45. Понятие группового канала

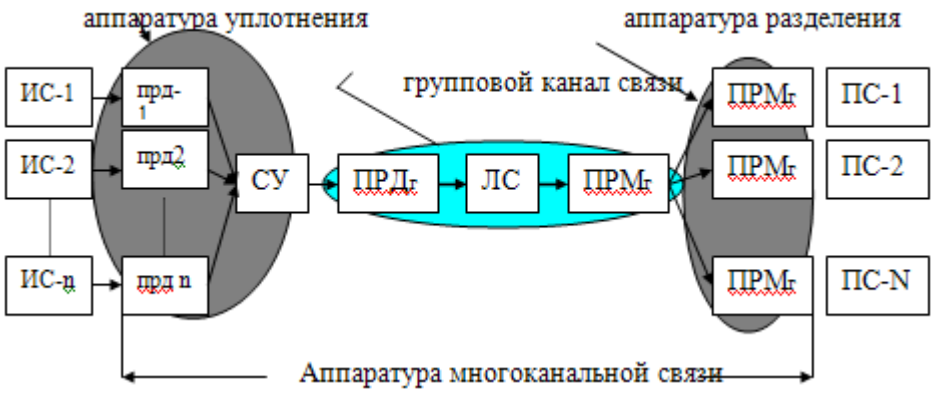


Рис.14. Структурная схема системы многоканальной связи

ИС- источник сообщений; ПС- получатель сообщений;

прд- канальный (индивидуальный) передатчик;прм- канальный (индивидуальный) приемник; СУ- суммирующее устройство; ПРДг – передатчик группового сигнала; ПРМг- приемник группового сигнала; ЛС – линия связи

46. Методы передачи дискретных сигналов в первичной полосе

47. Методы передачи данных.

<u>Физический уровень OSI</u>

Данный уровень содержит правила, которые определяют, как физически спроектированы сети, и как представляются биты в среде передачи.

Рис.*2.1.* Функциональная схема физического уровня

Элементы физического уровня:

- Типы соединений (двухточечные, многоточечные);
- Физическая топология;
- Передача сигналов (цифровая, аналоговая);
- Битовая синхронизация;
- Использование частотного диапазона (узкополосная, широкополосная передача);

Рекомендация X.200 и ISO 7498 определяет понятия назначения и выполняемые функции физического уровня.

Данные передаются в виде кодовых слов. Посылки (импульсы), отображающие разряды кодовых слов, могут передаваться последовательно и параллельно. В КС. как правило, используется последовательная передача, так как КС – дорогостоящее устройство. Последовательная передача– самый распространенный метод связи, требующий побитовой и блоковой синхронизации.

Различают двухточечные и многоточечные соединения:

Рис. 2.2. Типы двухточечных соединений

При двухточечном соединении корреспондирующие абоненты могу быть соединены выделенным каналом или через коммутируемую сеть (рис.2.2)

Пример многоточечного соединения представлен на рис.2.3.

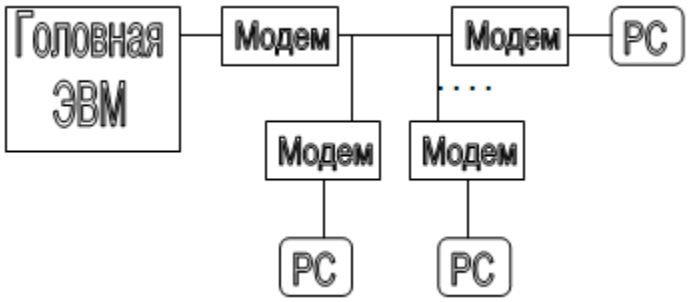


Рис. 2.3. Многоточечное соединение

При многоточечном соединении управление обменом, как правило, осуществляет головная ЭВМ. При двухточечном соединении в управлении обменом могут участвовать как одна так и обе станции.

При передаче данных по каналам связи применяются два типа физического кодирования — на основе синусоидального несущего колебания и на последовательности прямоугольных импульсов (посылок). Первый способ часто называется также *модуляцией,* подчеркивая тот факт, что кодирование осуществляется за счет изменения параметров аналогового сигнала. Второй обычно называют *цифровым кодированием.*

В настоящее время все чаще даже данные, изначально имеющие аналоговую форму - речь, телевизионное изображение — передаются по каналам связи в дискретном виде, то есть в виде последовательности единиц и нулей. Процесс представления] аналоговой информации в дискретной форме называется *дискретизацией.* Термины «модуляция» и «кодирование» часто используют как синонимы.

Методы передачи данных канального уровня

Канальный уровень обеспечивает передачу пакетов данных, поступающих от протоколов верхних уровней. Адрес узла назначения также указывает протокол верхнего уровня.

Протоколы канального уровня оформляют переданные им пакеты в кадры собственного формата, помещая указанный адрес назначения в одно из полей такого кадра, а также сопровождая кадр

контрольной суммой. Протокол канального уровня имеет локальный смысл, он предназначен для доставки кадров данных, как правило, в пределах локальных сетей с простой топологией связей и однотипной или близкой технологией, например в односегментных сетях Ethernet или же в многосегментных сетях Ethernet и Token Ring иерархической топологии, разделенных только мостами и коммутаторами. Во всех этих конфигурациях адрес назначения имеет локальный смысл для данной сети и не изменяется при прохождении кадра от узла-источника к узлу назначения. Возможность передавать данные между локальными сетями разных технологий связана с тем, что в этих технологиях используются адреса одинакового формата, к тому же производители сетевых адаптеров обеспечивают уникальность адресов независимо от технологии.

Обычно КУ в локальных сетях подразделяют на два подуровня:

1. Управление доступом к среде передач MAC (MEDIA ACCESS CONTROL);
2. Управление логическим соединением LLC (LOGICAL LINK CONTROL);

Уровень OSI	Элемент	Методы реализации
Канальный MAC	**Логич. тополог.** **Доступ к среде** **ПРД** **Адресация**	Шина, кольцо Состязание, маркер, опрос Физическое устройство (MAC-адрес[1])
Канальный LLC	Синхронизация передач Сервис соединений	Асинхронная Синхронная Управление потоком данных на LLC-уровне и контроль ошибок

Другой областью действия протоколов канального уровня являются связи типа “точка-точка” глобальных сетей, когда протокол канального уровня ответственен за доставку кадра непосредственному соседу. Адрес в этом случае не имеет принципиального значения, а на первый план выходит способность протокола восстанавливать искаженные и утерянные кадры, так как плохое качество территориальных каналов, особенно коммутируемых телефонных, часто требует выполнения подобных действий. Такие протоколы азывают линейными, они регламентируют передачу данных между соседними узлами в сети.

Наиболее существенными характеристиками метода передачи, а значит, и протокола, работающего на канальном, уровне, являются следующие:

• асинхронный/синхронный;

• символьно-ориентированный/бит-ориентированный;

• с предварительным установлением соединения/дейтаграммный;

• с обнаружением искаженных данных/без обнаружения;

• с обнаружением потерянных данных/без обнаружения;

1

• с восстановлением искаженных и потерянных данных/без восстановления;

• с поддержкой динамической компрессии данных/без поддержки.

Многие из этих свойств и для протоколов более высоких уровней.

48. Обнаружение ошибок. Восстановление искаженных и потерянных кадров.

Методы обнаружения ошибок

Все методы обнаружения ошибок основаны на передаче в составе кадра данных служебной избыточной информации, по которой можно судить с некоторой степенью вероятности о достоверности принятых данных. Эту служебную информацию принято называть *контрольной суммой* (или *последовательностью контроля кадра — Frame Check Sequence, FCS).* Контрольная сумма вычисляется как функция от основной информация, причем необязательно только путем суммирования. Принимающая сторона повторно вычисляет контрольную сумму кадра по известному алгоритму и в случае ее совпадения с контрольной суммой, вычисленной передающей стороной, делает вывод о том, что данные были переданы через сеть корректно.

Существует несколько распространенных алгоритмов вычисления контрольной суммы, отличающихся вычислительной сложностью и способностью обнаруживать ошибки в данных.

Контроль по паритету представляет собой наиболее простой метод контроля данных. В то же время это наименее мощный алгоритм контроля, так как с его помощью можно обнаружить только одиночные ошибки в проверяемых данных. Метод заключается суммировании по модулю 2 всех бит контролируемой информации. Например, для данных 100101011 результатом контрольного суммирования будет значение 1. Результат суммирования также представляет собой один бит данных, который пересылается вместе с контролируемой информацией. Искажение какого либо одного бита обнаруживае6тся. Однако двойная ошибка, например 110101010, будет неверно принята за корректные данные. Поэтому контроль по паритету применяется к небольшим порциям данных,, как правило, к каждому байту, что дает коэффициент избыточности для этого метода 1/8. Метод редко применяется в вычислительных сетях из-за его большой избыточности и невысоких диагностических способностей.

Вертикальный и горизонтальный контроль по паритету представляет собой модификацию описанного выше метода. Его отличие состоит в том, что исходные данных! рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы. Этот метод обнаруживает большую часть двойных ошибок, однако обладает еще большей избыточностью. На практике сейчас также почти не применяется.

Циклический избыточный контроль (Cyclic Redundancy Check, CRC) является в настоящее время наиболее популярным методом контроля в вычислительных сетях (и не только в сетях, например, этот метод широко применяется при записи данных на диски и дискеты). Метод основан на рассмотрении исходных данных виде одного многоразрядного двоичного числа. Например, кадр стандарта Ethernet состоящий из 1024 байт, будет рассматриваться как одно число, состоящее и 8192 бит. В качестве контрольной информации рассматривается остаток от деления этого числа на известный делитель R. Обычно в качестве делителя выбирается семнадцати- или тридцати трехразрядное число, чтобы остаток от деления длину 16 разрядов (2 байт) или 32 разряда (4 байт). При получении кадра данных снова вычисляется остаток от деления на тот же делитель R, но при этом к данным кадра добавляется и

содержащаяся в нем контрольная сумма. Если остаток от деления на R равен нулю, то делается вывод об отсутствии ошибок в получение кадре, в противном случае кадр считается искаженным.

Этот метод обладает более высокой вычислительной сложностью, но его диагностические возможности гораздо выше, чем у методов контроля по паритету. Метод CRC обнаруживает все одиночные ошибки, двойные ошибки и ошибки в нечетном числе бит, Метод обладает также невысокой степенью избыточности. Например, для кадра Ethernet размером в 1024 байт контрольная информация длиной в 4 байт составляет только 0,4 %. .

Методы восстановления искаженных и потерянных кадров

Методы коррекции ошибок в вычислительных сетях основаны на повторной передаче кадра данных в том случае, если кадр теряется и не доходит до адресата или приемник обнаружил в нем искажение информации. Чтобы убедиться в необходимости повторной передачи данных, отправитель нумерует отправляемые кадры и для каждого кадра ожидает от приемника так называемой *положительной квитанции* — служебного кадра, извещающего о том, что исходный кадр был получен и данные в нем оказались корректными. Время этого ожидания ограничено — при отправке каждого кадра передатчик запускает таймер, и, если по его истечении положительная квитанция на получена, кадр считается утерянным. Приемник в случае получения кадра с искаженными данными может отправить *отрицательную квитанцию* — явное указание на то, что данный кадр нужно передать повторно.

Существуют два подхода к организации процесса обмена квитанциями: с простоями и с организацией “окна”.

Метод с простоями (Idle Source) требует, чтобы источник, пославший кадр, ожидал получения квитанций (положительной или отрицательной) от приемника и только после этого посылал следующий кадр (или повторял искаженный). Если же квитанция не приходит в течение тайм-аута, то кадр (или квитанция) считается утерянным и его передача повторяется. При этом методе производительность обмена данными существенно снижается, — хотя передатчик и мог бы послать следующий кадр сразу же после отправки предыдущего, он обязан ждать прихода квитанции. Снижение производительности этого метода коррекции особенно заметно на низкоскоростных каналах связи, то есть в территориальных сетях.

Второй метод называется методом *скользящего* окна *(sliding window).* В этом методе для повышения коэффициента использования линии источнику разрешается передать некоторое количество кадров в непрерывном режиме, то есть в максимально возможном для источника темпе, без получения на эти кадры положительных ответных квитанций. Количество W кадров, которые разрешается передавать таким образом, называется размером окна.

В начальный момент, когда еще не послано ни одного кадра, окно определяет диапазон кадров с номерами от 1 до W включительно. Источник начинает передавать кадры и получать в ответ квитанции. Для простоты предположим, что квитанции поступают в той же последовательности, что и кадры, которым они соответствуют. В момент ti при получении первой квитанции K1 окно сдвигается на одну позицию, определяя новый диапазон от 2 до (W+1).

Процессы отправки кадров и получения квитанций идут достаточно независимо друг от друга. Рассмотрим произвольный момент времени tn, когда источник получил квитанцию на кадр с номером n. Окно сдвинулось вправо и определило диапазон разрешенных к передаче кадров от (n+1) до (W+n). Все множество кадров, выходящих из источника, можно разделить на перечисленные ниже группы.

• *Кадры с номерами от 1 до n.* уже были отправлены и квитанции на них получены, то есть они находятся за пределами окна слева.

• *Кадры, наминая с номера (n+1) и кончая номером (W+n),* находятся в пределах окна и потому могут быть отправлены не дожидаясь прихода какой-либо квитанции. Этот диапазон может быть разделен еще на два поддиапазона:

• кадры с номерами от (n +1) до m, которые уже отправлены, но квитанции на них еще не получены;

• кадры с номерами от m до (W+n), которые пока не отправлены, хотя запрета на это нет.

• *Все кадры с номерами, большими или равными (W+n+1),* находятся за пределами окна справа и поэтому пока не могут быть отправлены.

Каждый раз, когда приходит квитанция, окно сдвигается влево, но его размер при этом не меняется и остается равным W. Заметим, что хотя в данном примере размер окна в процессе передачи остается постоянным, в реальных протоколах (например, TCP) можно встретить варианты данного алгоритма с изменяющимся размером окна.

Итак, при отправке кадра с номером n источнику разрешается передать еще W-1 кадров до получения квитанции на кадр n, так что в сеть последним уйдет кадр с номером (W+n-1). Если же за это время квитанция на кадр n так и не пришла, то процесс передачи приостанавливается, и по истечении некоторого тайм-аута кадр n (или квитанция на него) считается утерянным, и он передается снова.

Если же поток квитанций поступает более-менее регулярно, в пределах допуска в W кадров, то скорость обмена достигает максимально возможной величины для данного канала и принятого протокола.

Метод скользящего окна более сложен в реализации, чем метод с простоями, так как передатчик должен хранить в буфере все кадры, на которые пока не получены положительные квитанции. Кроме того, требуется отслеживать несколько параметров алгоритма: размер окна W, номер кадра, на который получена квитанция, номер кадра, который еще можно передать до получения новой квитанции.

Приемник может не посылать квитанции на каждый принятый корректный кадр. Если несколько кадров пришли почти одновременно, то приемник может послать квитанцию только на последний кадр. При этом подразумевается, что все предыдущие кадры также дошли благополучно.

Некоторые методы используют отрицательные квитанции. Отрицательные квитанции бывают двух типов — групповые и избирательные. Групповая квитанция содержит номер кадра, начиная с которого нужно повторить передачу всех кадров, отправленных передатчиком в сеть. Избирательная отрицательная квитанция требует повторной передачи только одного кадра.

Метод скользящего окна реализован во многих протоколах: LLC2, LAP-B, X.25, TCP, Novell NCP Burst Mode.

Метод с простоями является частным случаем метода скользящего окна, когда размер окна равен единице.

Метод скользящего окна имеет два параметра, которые могут заметно влиять на эффективность передачи данных между передатчиком и приемником, — размер окна и величина тайм-аута ожидания квитанции. В надежных сетях, когда кадры искажаются и теряются редко, для повышения скорости обмена данными размер окна нужно увеличивать, так как при этом передатчик будет посылать кадры с меньшими паузами. В ненадежных сетях размер окна следует уменьшать, так как при частых потерях и искажениях кадров резко возрастает объем вторично передаваемых через сеть кадров, а значит, пропускная способность сети будет расходоваться во многом вхолостую — полезная пропускная способность сети будет падать.

Выбор тайм-аута зависит не от надежности сети, а от задержек передачи кадров сетью.

Во многих реализациях метода скользящего окна величина окна и тайм-аут выбираются адаптивно, в зависимости от текущего состояния сети.

49. Линейные протоколы управления потоком данных

50. Компрессия данных.

Компрессия (сжатие) данных применяется для сокращения времени **их** передачи. Так как на компрессию данных передающая сторона тратит дополнительное время, к которому нужно еще прибавить аналогичные затраты времени на декомпрессию этих данных принимающей стороной, то выгоды от сокращения времени на передачу сжатых данных обычно бывают заметны только для низкоскоростных каналов. Этот порог скорости для современной аппаратуры составляет около 64 Кбит/с. Многие программные и аппаратные средства сети способны выполнять *динамическую компрессию* данных в отличие от статической, когда данные предварительно компрессируются (например, с помощью популярных архиваторов типа WinZip), а уже затем отсылаются в сеть.

На практике может использоваться ряд алгоритмов компрессии, каждый из которых применим к определенному типу данных. Некоторые модемы (называемые интеллектуальными) предлагают *адаптивную компрессию,* при которой в зависимости от передаваемых данных выбирается определенный алгоритм компрессии. Рассмотрим некоторые из общих алгоритмов компрессии данных

Десятинная упаковка. Когда данные состоят только из чисел, значительную экономию можно получить путем уменьшения количества используемых на цифру бит с 7 до 4, используя простое двоичное кодирование десятичных цифр вместо кода ASCII. Просмотр таблицы ASCII показывает, что старшие три бита всех кодов десятичных цифр содержат комбинацию 011. Если все данные в кадре информации состоят из десятичных цифр, то, поместив в заголовок кадра соответствующий управляющий символ, можно существенно сократить длину кадра.

Относительное кодирование. Альтернативой десятичной упаковке при передаче числовых данных с небольшими отклонениями между последовательными цифрами является передача только этих отклонений вместе с известным опорным значением. Такой метод используется, в частности, в рассмотренном выше методе цифрового кодирования голоса ADPCM, передающем в каждом такте только разницу между соседними замерами голоса.

Символьное подавление. Часто передаваемые данные содержат большое количество повторяющихся байт. Например, при передаче черно-белого изображения черные поверхности будут порождать большое количество нулевых значений, а максимально освещенные участки изображения — большое количество байт, состоящих из всех единиц. Передатчик сканирует последовательность передаваемых байт и, если обнаруживает последовательность из трех или более одинаковых байт, заменяет ее специальной трехбайтовой последовательностью, в которой указывает значение байта, количество его повторений, а также отмечает начало этой последовательности специальным управляющим символом.

Коды переменной длины. В этом методе кодирования используется тот факт, что не все символы в передаваемом кадре встречаются с одинаковой частотой. Поэтому во многих схемах кодирования коды часто встречающихся символов заменяют кодами меньшей длины, а редко встречающихся — кодами большей длины. Такое кодирование называется также статистическим кодированием. Из-за того, что символы имеют различную длину, для передачи кадра возможна только бит-ориентированная передача.

При *статистическом кодировании* коды выбираются таким образом, чтобы при анализе последовательности бит можно было бы однозначно определить соответствие определенной порции бит тому или иному символу или же запрещенной комбинации бит. Если данная последовательность бит представляет собой запрещенную комбинацию, то необходимо к ней добавить еще один бит и повторить анализ. Например, если при неравномерном кодировании для наиболее часто встречающегося символа «Р» выбран код 1, состоящий из одного бита, то значение 0 однобитного кода будет запрещенным. Иначе мы сможем закодировать только два символа. Для другого часто встречающегося символа «О» можно использовать код 01, а код 00 оставить как запрещенный. Тогда для символа «А> можно выбрать код 001, для символа <П> — код 0001 и т. п.

Вообще, неравномерное кодирование наиболее эффективно, когда неравномерность распределения частот передаваемых символов достаточна велика, как при передаче длинных текстовых строк. Напротив, при передаче двоичных данных, например кодов программ, оно малоэффективно, так как 8-битовые коды при этом распределены почти равномерно.

Одним из наиболее распространенных алгоритмов, на основе которых строятся неравномерные коды, является алгоритм Хафмана, позволяющий строить коды автоматически, на основании известных частот символов. Существуют адаптивные модификации метода Хафмана, которые позволяют строить дерево кодов «на ходу», по мере поступления данных от источника.

Многие модели коммуникационного оборудования, такие как модемы, мосты, коммутаторы и маршрутизаторы, поддерживают протоколы динамической компрессии, позволяющие сократить объем передаваемой информации в 4, а иногда и в 8 раз. В таких случаях говорят, что протокол обеспечивает коэффициент сжатия 1:4 или 1:8. Существуют стандартные протоколы компрессии, например V.42bis, а также большое количество нестандартных, фирменных протоколов. Реальный коэффициент компрессии зависит от типа передаваемых данных, так, графические и текстовые данные обычно сжимаются хорошо, а коды программ — хуже.

Резюме

• Основной задачей протоколов канального уровня является доставка кадра узлу назначения в сети определенной технологии и достаточно простой топологии.

• Асинхронные протоколы разрабатывались для обмена данными между низкоскоростными старт-стопными устройствами: телетайпами, алфавитно-цифровыми терминалами и т. п. В этих протоколах для управления обменом данными используются не кадры, а отдельные символы из нижней части кодовых таблиц ASCII или EBCDIC. Пользовательские данные могут оформляться в кадры, но байты в таких кадрах всегда отделяются друг от друга стартовыми и стоповыми сигналами.

• Синхронные протоколы посылают кадры как для отправки пользовательских данных, так и для управления обменом.

• В зависимости от способа выделения начала и конца кадра синхронные протоколы делятся на символьно-ориентированные и бит-ориентированные. В первых для этой цели используются символы кодов ASCII или EBCDIC, а в последних — специальный набор бит, называемый флагом. Бит-ориентированные протоколы более рационально расходуют поле данных кадра, так как для исключения из него значения, совпадающего с 4>лагом, добавляют к нему только один дополнительный бит, а символьно-ориентированные протоколы добавляют целый символ.

• В дейтаграммных протоколах отсутствует процедура предварительного установления соединения, и за счет этого срочные данные отправляются в сеть без задержек.

• Протоколы с установлением соединения могут обладать многими дополнительными свойствами, отсутствующими у дейтаграммных протоколов. Наиболее часто в них реализуется такое свойство, как способность восстанавливать искаженные и потерянные кадры.

• Для обнаружения искажений наиболее популярны методы, основанные на циклических избыточных кодах (CRC), которые выявляют многократные ошибки.

• Для восстановления кадров используется метод повторной передачи на основе квитанций. Этот метод работает по алгоритму с простоями источника, а также по алгоритму скользящего окна.

• Для повышения полезной скорости передачи данных в сетях применяется динамическая компрессия данных на основе различных алгоритмов. Коэффициент сжатия зависит от типа данных и применяемого алгоритма и может колебаться в пределах **от** 1:2 до 1:8.