

Сетевые интерфейсы

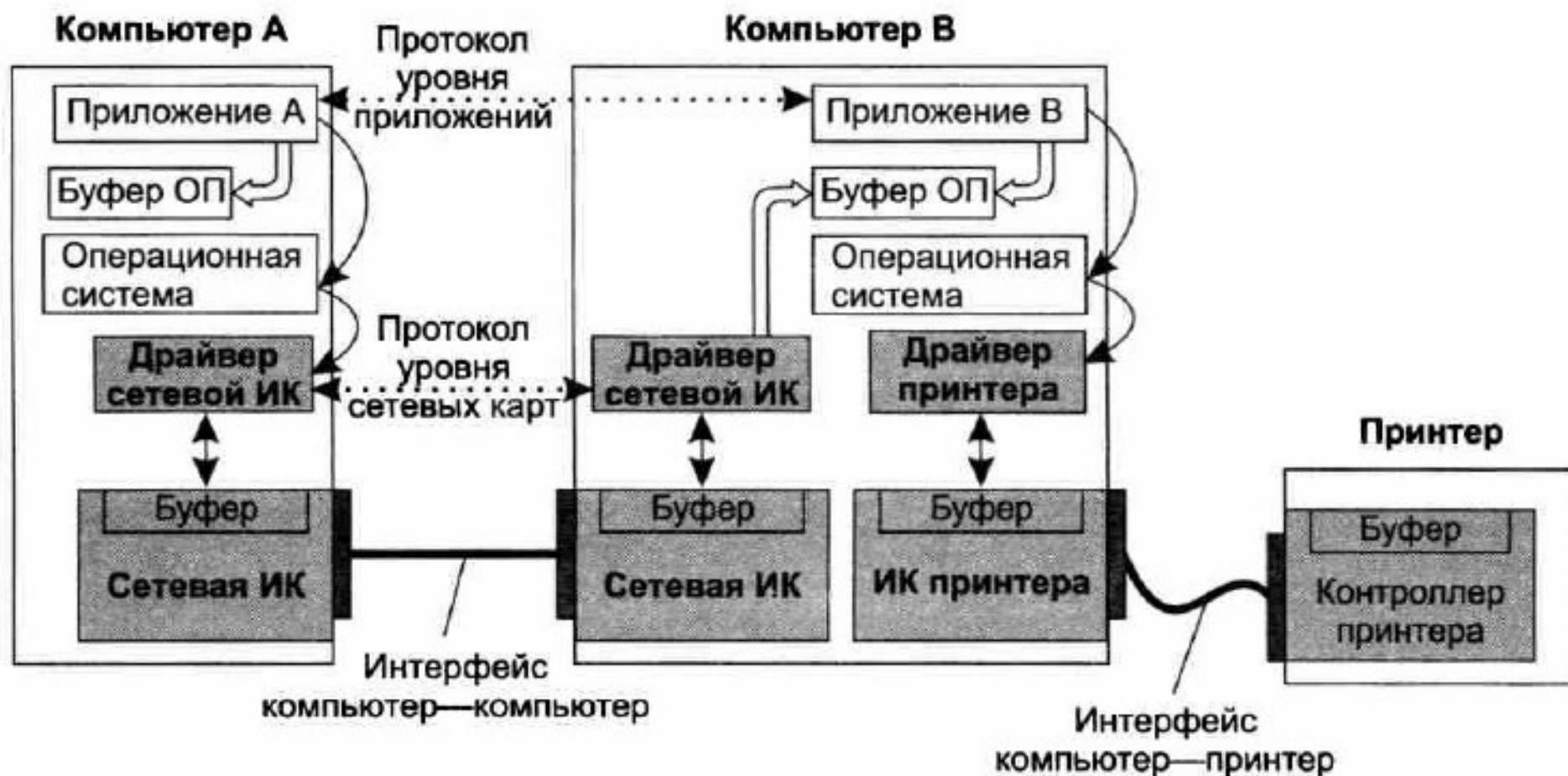
- Интерфейс — в широком смысле — формально определенная логическая и/или физическая граница между взаимодействующими независимыми объектами. Интерфейс задает параметры, процедуры и характеристики взаимодействия объектов.

Сетевые интерфейсы

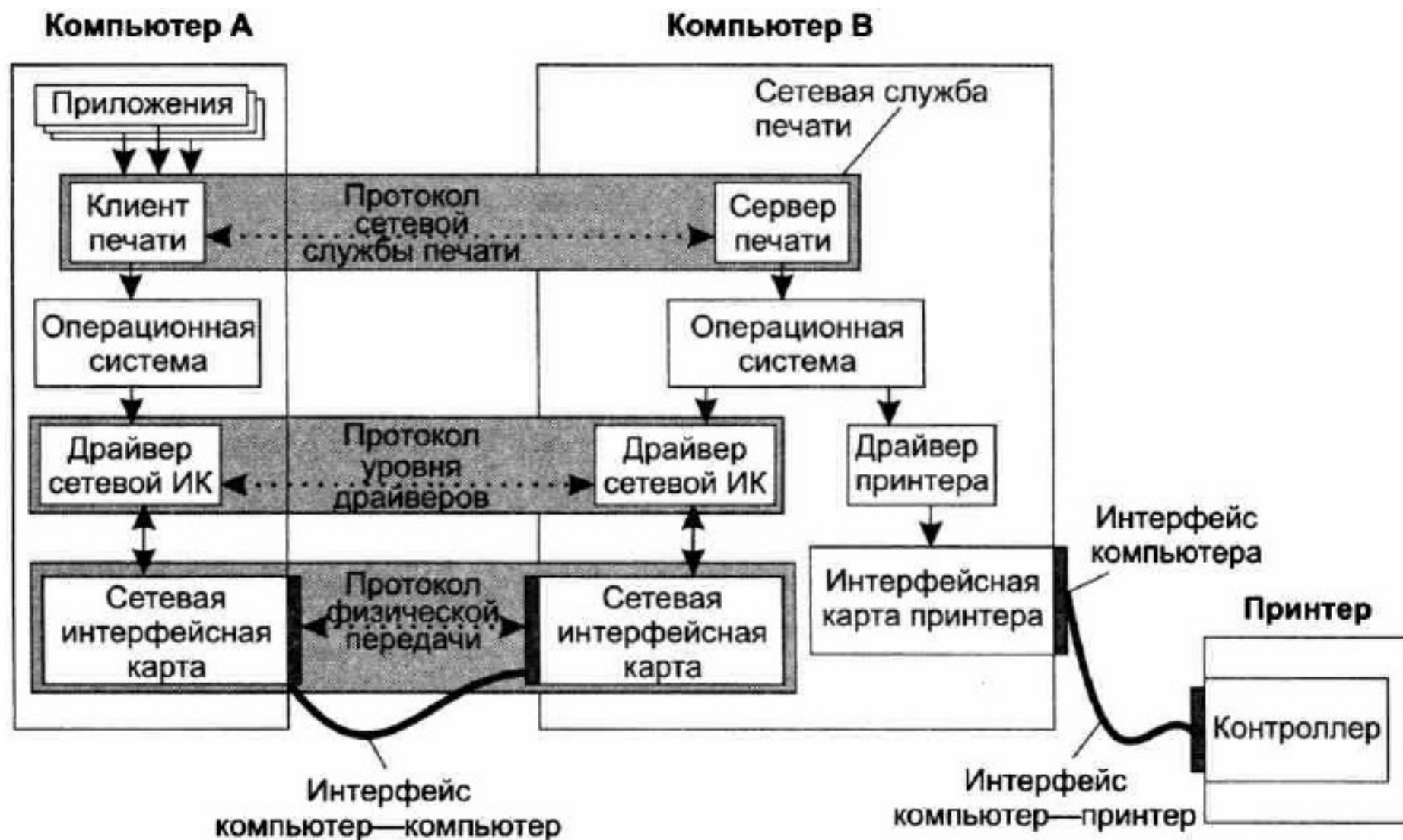
Разделяют физический и логический интерфейсы.

- **Физический интерфейс** (называемый также портом) определяется набором электрических связей и характеристиками сигналов. Обычно он представляет собой разъем с набором контактов, каждый из которых имеет определенное назначение, например это может быть группа контактов для передачи данных, контакт синхронизации данных и т. п. Пара разъемов соединяется кабелем, состоящим из набора проводов, каждый из которых соединяет соответствующие контакты. В таких случаях говорят о создании линии, или канала, связи между двумя устройствами.
- **Логический интерфейс** (называемый также протоколом) — это набор информационных сообщений определенного формата, которыми обмениваются два устройства или две программы, а также набор правил, определяющих логику обмена этими сообщениями.

Сетевые интерфейсы



Сетевые службы и сервисы



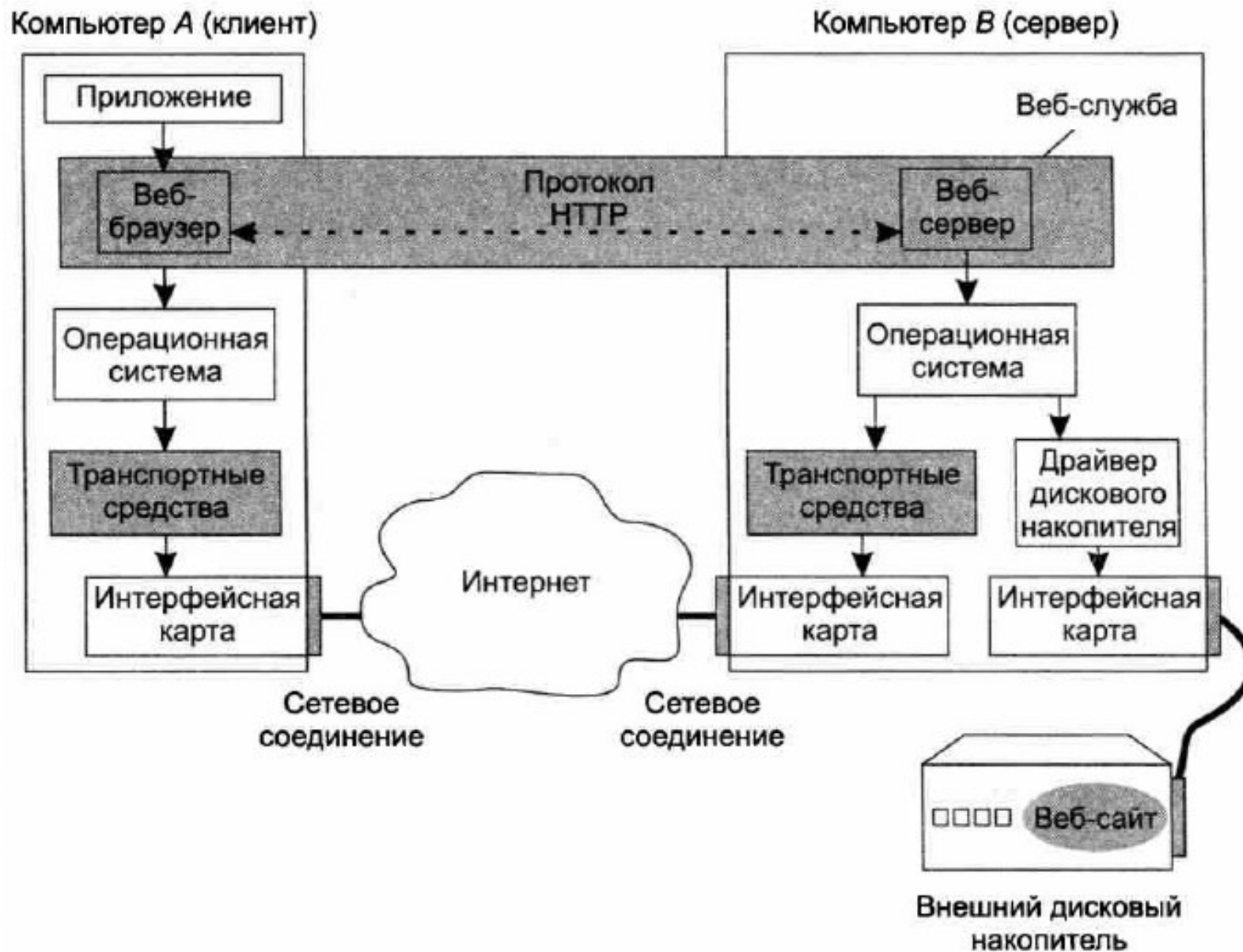
Сетевые службы и сервисы

Клиент — это модуль, предназначенный для формирования и передачи сообщений-запросов к ресурсам удаленного компьютера от разных приложений с последующим приемом результатов из сети и передачей их соответствующим приложениям.

Сервер — это модуль, который постоянно ожидает прихода из сети запросов от клиентов и, приняв запрос, пытается его обслужить, как правило, с участием локальной ОС; один сервер может обслуживать запросы сразу нескольких клиентов (поочередно или одновременно).

Пара клиент—сервер, предоставляющая доступ к конкретному типу ресурса компьютера через сеть, образует **сетевую службу**.

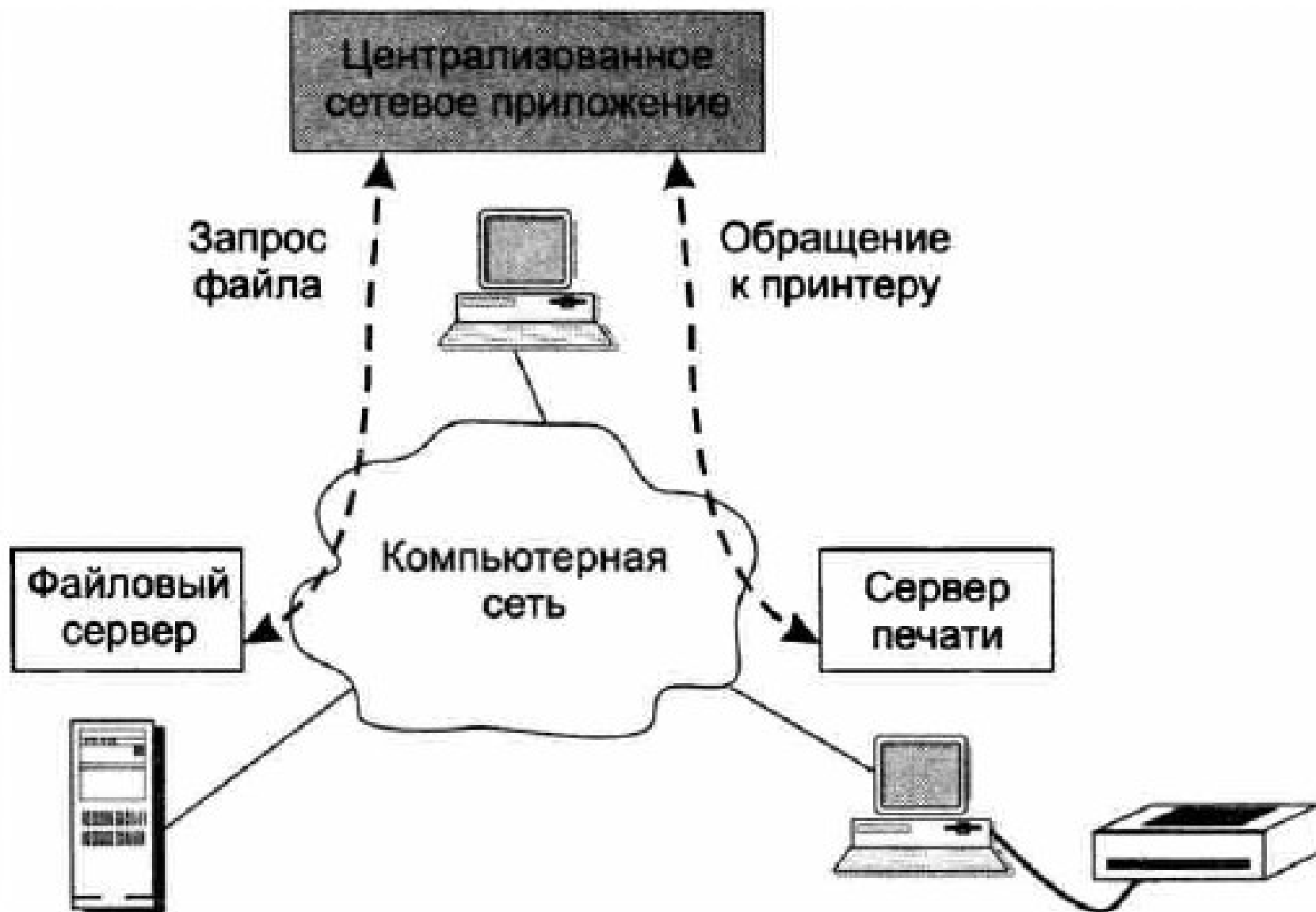
Веб-служба



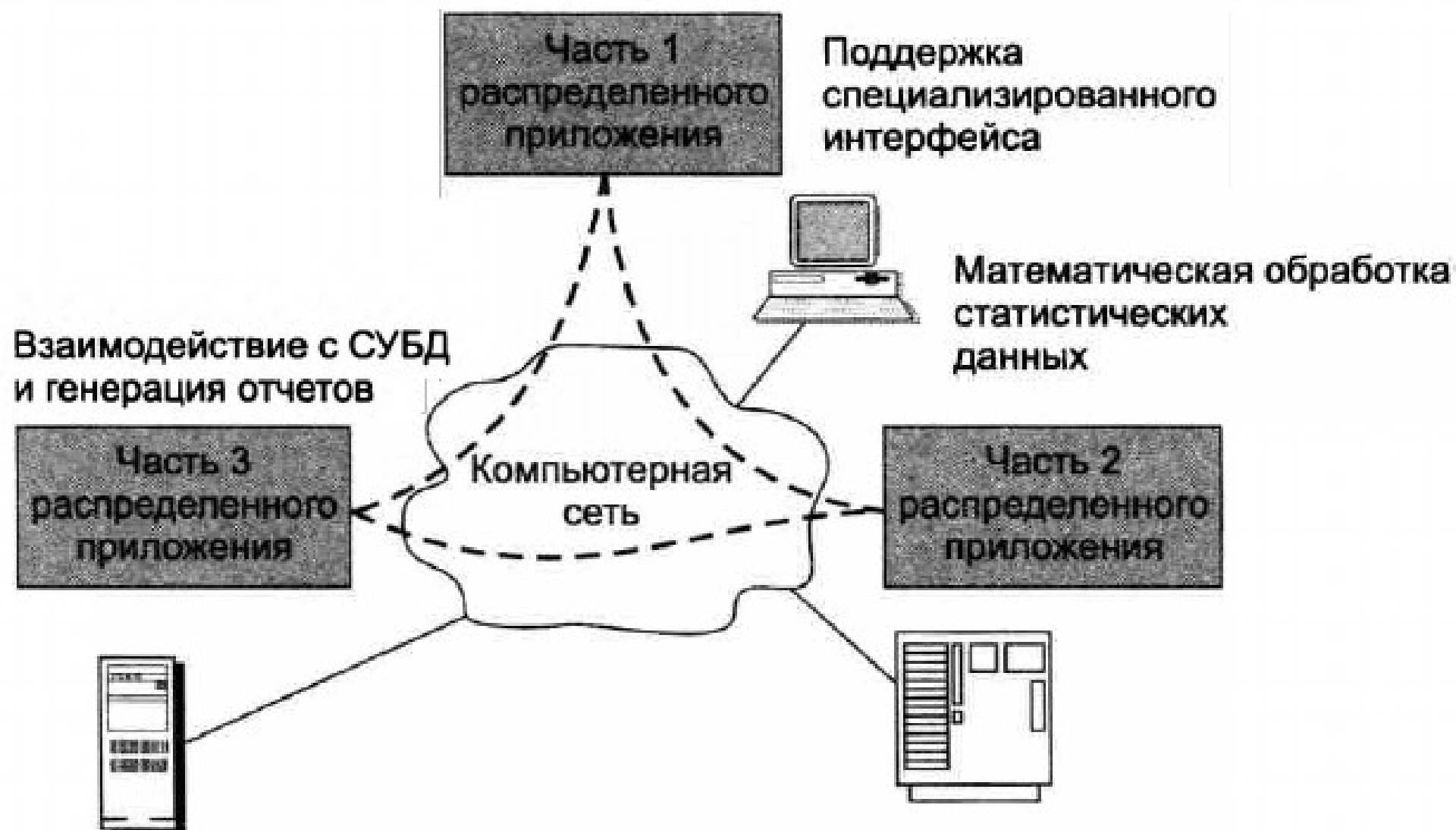
Локальное приложение



Централизованное сетевое приложение

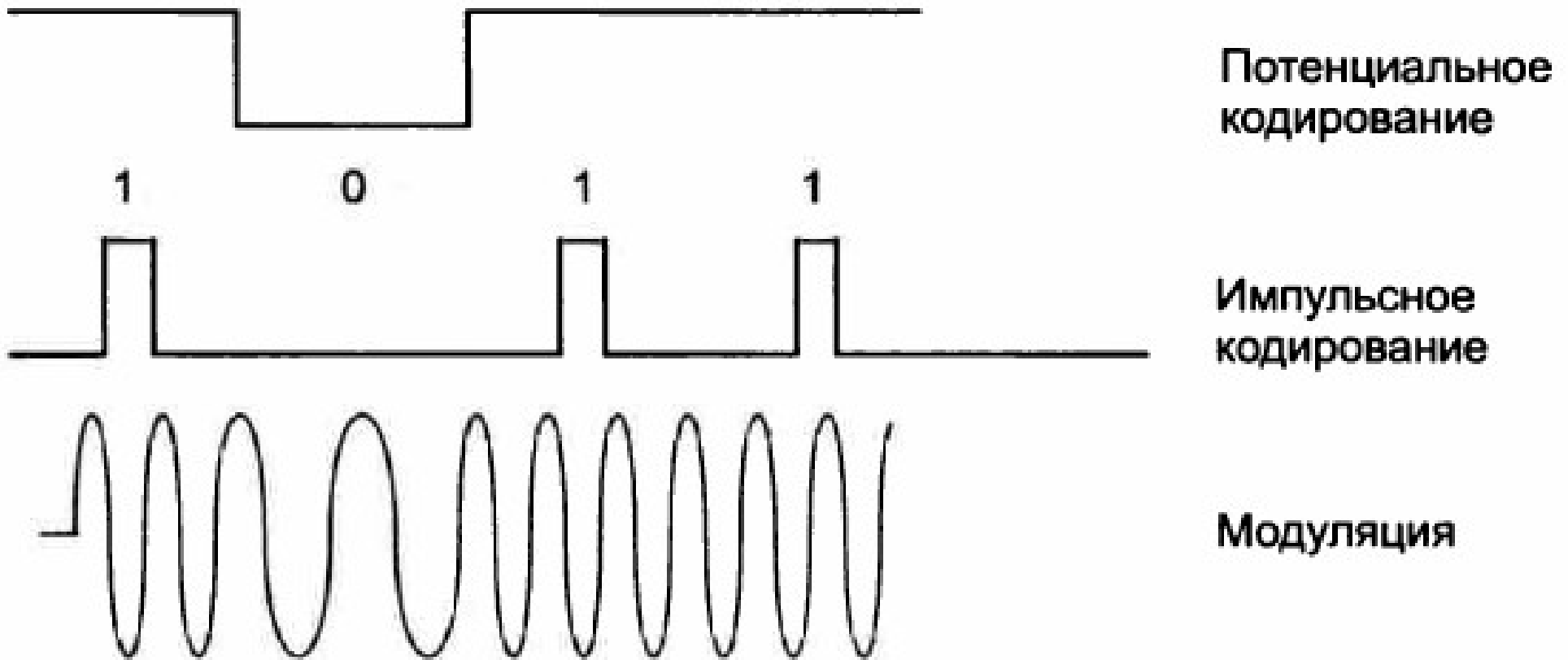


Распределенное (сетевое) приложение



Физическая передача данных по линиям связи. Кодирование

Представление данных в виде электрических или оптических сигналов называется **кодированием**.



Характеристики физических каналов

Предложенная нагрузка — это поток данных, поступающий от пользователя на вход сети. Предложенную нагрузку можно характеризовать скоростью поступления данных в сеть в битах в секунду (или килобитах, мегабитах и т. д.).

Скорость передачи данных (information rate, или throughput, оба английских термина используются равноправно) — это фактическая скорость потока данных, прошедшего через сеть. Эта скорость может быть меньше, чем скорость предложенной нагрузки, так как данные в сети могут искажаться или теряться.

Емкость канала связи (capacity), называемая также пропускной способностью, представляет собой максимально возможную скорость передачи информации по каналу.

Характеристики физических каналов

Полоса пропускания (bandwidth) — этот термин может ввести в заблуждение, потому что он используется в двух разных значениях. Во-первых, с его помощью могут характеризовать среду передачи. В этом случае он означает ширину полосы частот, которую линия передает без существенных искажений. Во-вторых, термин «полоса пропускания» используется как синоним термина емкость канала связи. В первом случае полоса пропускания измеряется в герцах (Гц), во втором — в битах в секунду.

Характеристики физических каналов

Дуплексный канал обеспечивает одновременную передачу информации в обоих направлениях.

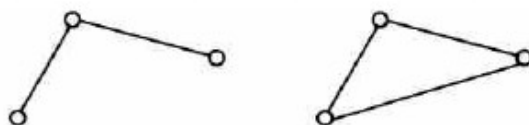
Дуплексный канал может состоять из двух физических сред, каждая из которых используется для передачи информации только в одном направлении.

Полудуплексный канал также обеспечивает передачу информации в обоих направлениях, но не одновременно, а по очереди.

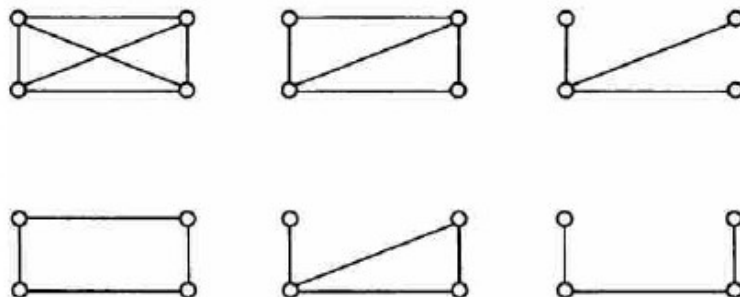
Симплексный канал позволяет передавать информацию только в одном направлении. Часто дуплексный канал состоит из двух симплексных каналов.

Топология физических связей

Под **топологией сети** понимается конфигурация графа, вершинам которого соответствуют конечные узлы сети (например, компьютеры) и коммуникационное оборудование (например, маршрутизаторы), а ребрам — физические или информационные связи между вершинами.



а



б

Топология физических связей

а) Полносвязная

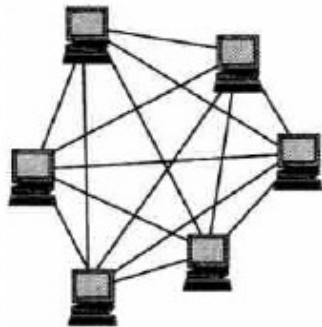
б) Ячеистая

в) Кольцевая

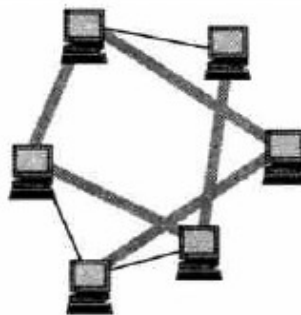
г) Звездообразная

д) Иерархическая звезда, дерево

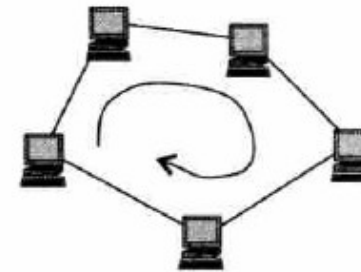
е) Общая шина



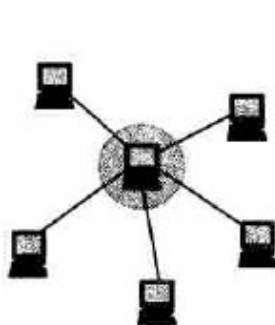
а



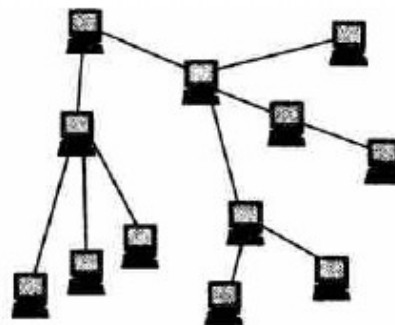
б



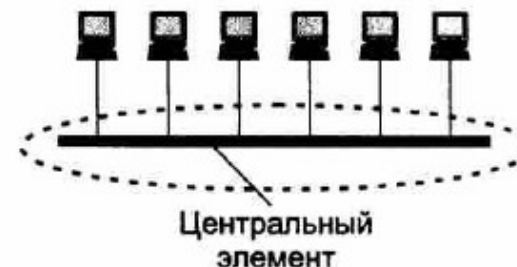
в



г



д



е

Адресация узлов сети

Один компьютер может иметь несколько сетевых интерфейсов. Например, для создания полносвязной структуры из N компьютеров необходимо, чтобы у каждого из них имелся N - 1 интерфейс.

По количеству адресуемых интерфейсов адреса можно классифицировать следующим образом:

- **уникальный адрес** (unicast) используется для идентификации отдельных интерфейсов;
- **групповой адрес** (multicast) идентифицирует сразу несколько интерфейсов, поэтому данные, помеченные групповым адресом, доставляются каждому из узлов, входящих в группу;
- данные, направленные по **широковещательному адресу** (broadcast), должны быть доставлены всем узлам сети;
- **адрес произвольной рассылки** (anycast), определенный в новой версии протокола IPv6, так же как и групповой адрес, задает группу адресов, однако данные, посланные по этому адресу, доставляются не всем узлам данной группы, а только одному из них. Выбор этого узла осуществляется в соответствии с некоторыми правилами предпочтения.

Адреса могут быть **числовыми** (например, 129.26.255.255 или 81.la.ff.ff) и **символьными** (site.domen.ru, willi-winki).

Адресация узлов сети

Множество всех адресов, которые являются допустимыми в рамках некоторой схемы адресации, называется **адресным пространством**. Адресное пространство может иметь плоскую (линейную) или иерархическую организацию.

- При **плоской организации** множество адресов никак не структурировано. Примером плоского числового адреса является **MAC-адрес**, предназначенный для однозначной идентификации сетевых интерфейсов в локальных сетях.
- При иерархической организации адресное пространство структурируется в виде вложенных друг в друга подгрупп, которые, последовательно сужая адресуемую область, в конце концов, определяют отдельный сетевой интерфейс.

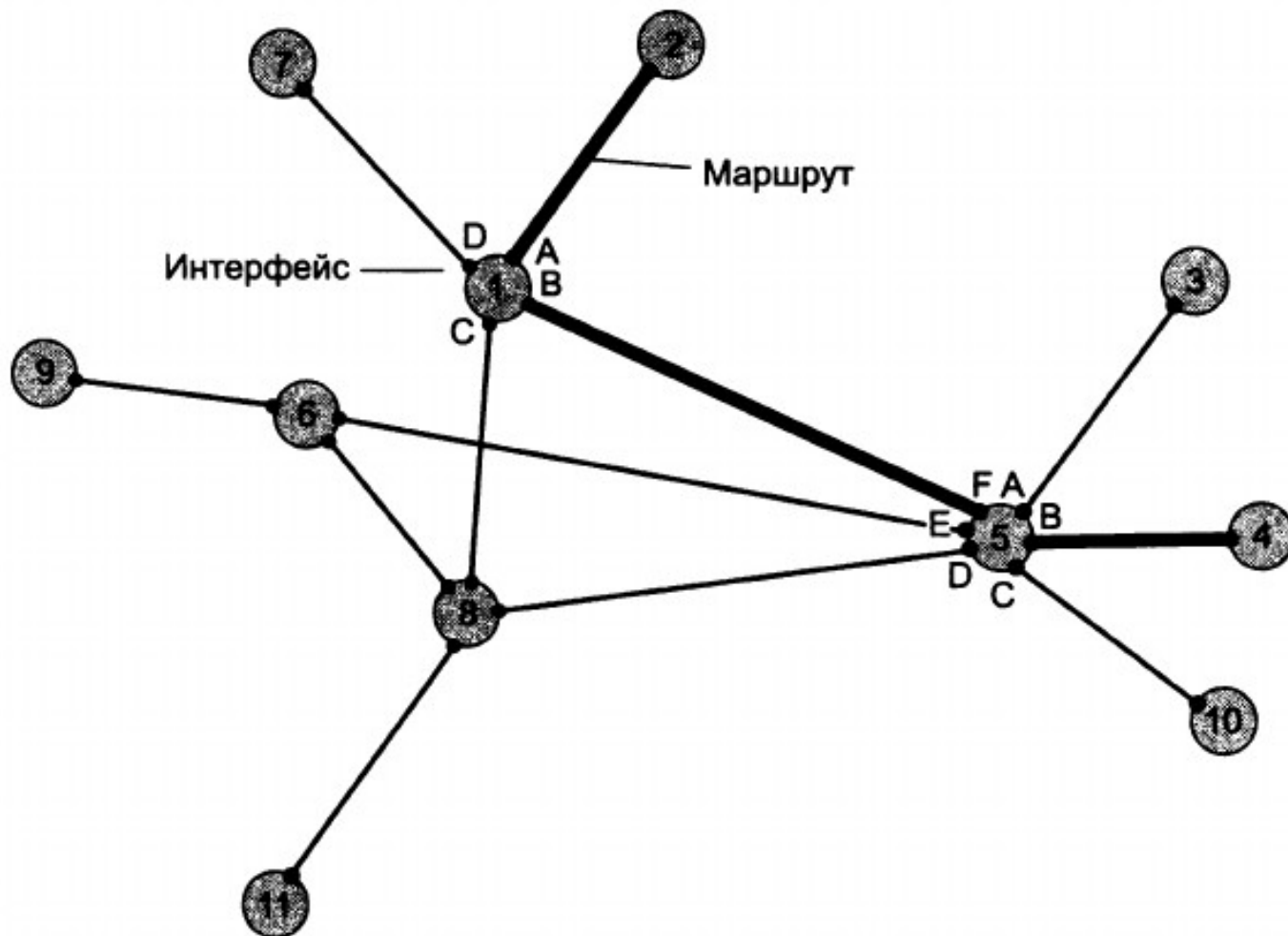
Адресация узлов сети

А для преобразования адресов из одного вида в другой используются специальные вспомогательные протоколы, которые называют **протоколами разрешения адресов**.

- При **централизованном подходе** в сети выделяется один или несколько компьютеров (серверов имен), в которых хранится таблица соответствия имен различных типов, например символьных имен и числовых адресов.
- При **распределенном подходе** каждый компьютер сам хранит все назначенные ему адреса разного типа. посылает ответ, содержащий искомый аппаратный адрес. Такая схема использована в **протоколе разрешения адресов** (Address Resolution Protocol, ARP) стека TCP/IP.

Коммутация

Соединение конечных узлов через сеть транзитных узлов называют коммутацией. Последовательность узлов, лежащих на пути от отправителя к получателю, образует **маршрут**.



Коммутация

Информационным потоком, или потоком данных, называют непрерывную последовательность данных, объединенных набором общих признаков, выделяющих эти данные из общего сетевого трафика.

Метка потока — это особый тип признака. Она представляет собой некоторое число, которое несут все данные потока.

Глобальная метка назначается данным потока и не меняет своего значения на всем протяжении его пути следования от узла источника до узла назначения, таким образом, она уникально определяет поток в пределах сети. В некоторых технологиях используются **локальные метки потока**, динамически меняющие свое значение при передаче данных от одного узла к другому.

Маршрутизация

Задача маршрутизации в свою очередь включает в себя две подзадачи:

- Определение маршрута;
- Оповещение сети о выбранном маршруте.

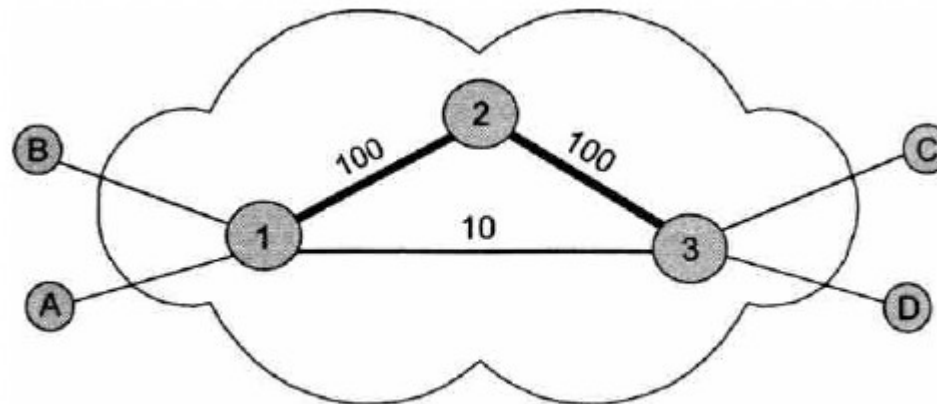


Рис. 2.13. Выбор маршрута

Абстрактная оценка условного «расстояния» между двумя узлами сети называется **метрикой**. Так, для измерения длины маршрута могут быть использованы разные метрики — количество транзитных узлов, как в предыдущем примере, линейная протяженность маршрута и даже его стоимость в денежном выражении.

Маршрутизация

«Каждый раз, когда в устройство поступят данные, относящиеся к потоку n , их следует передать для дальнейшего продвижения на интерфейс if1». Каждое подобное сообщение о маршруте обрабатывается транзитным устройством, в результате создается новая запись в **таблице коммутации** (называемой также **таблицей маршрутизации**).

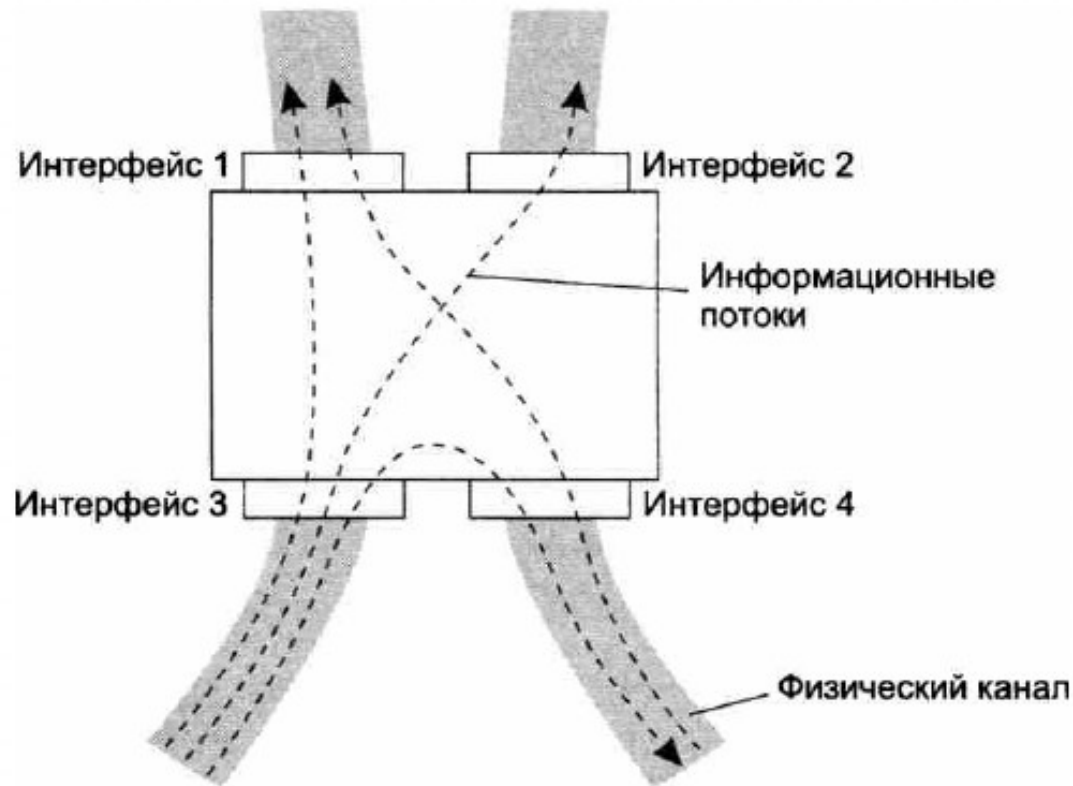
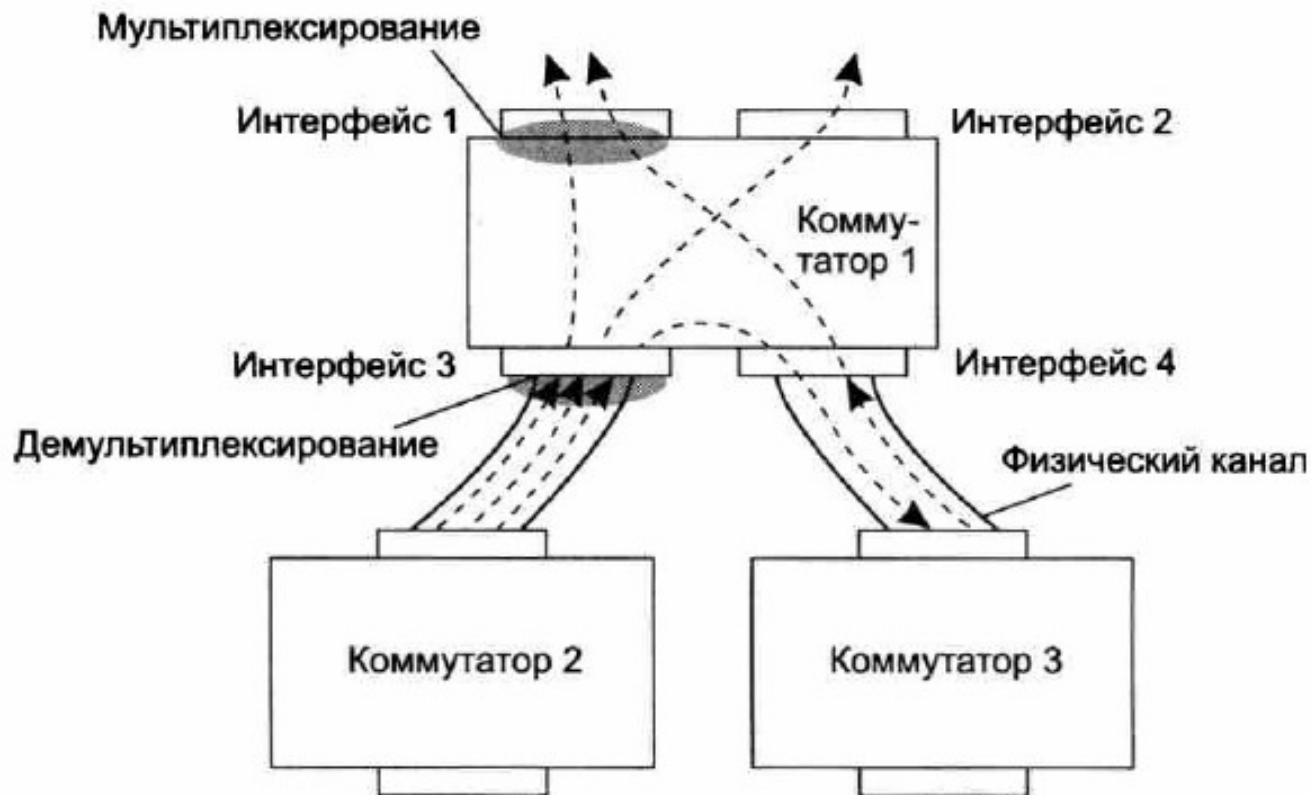


Рис. 2.14. Коммутатор

Маршрутизация

Демультимплексирование — разделение суммарного потока на несколько составляющих его потоков.

Мультиплексирование (агрегирование) — образование из нескольких отдельных потоков общего агрегированного потока, который передается по одному физическому каналу связи.



Коммутация каналов и пакетов. Коммутация каналов

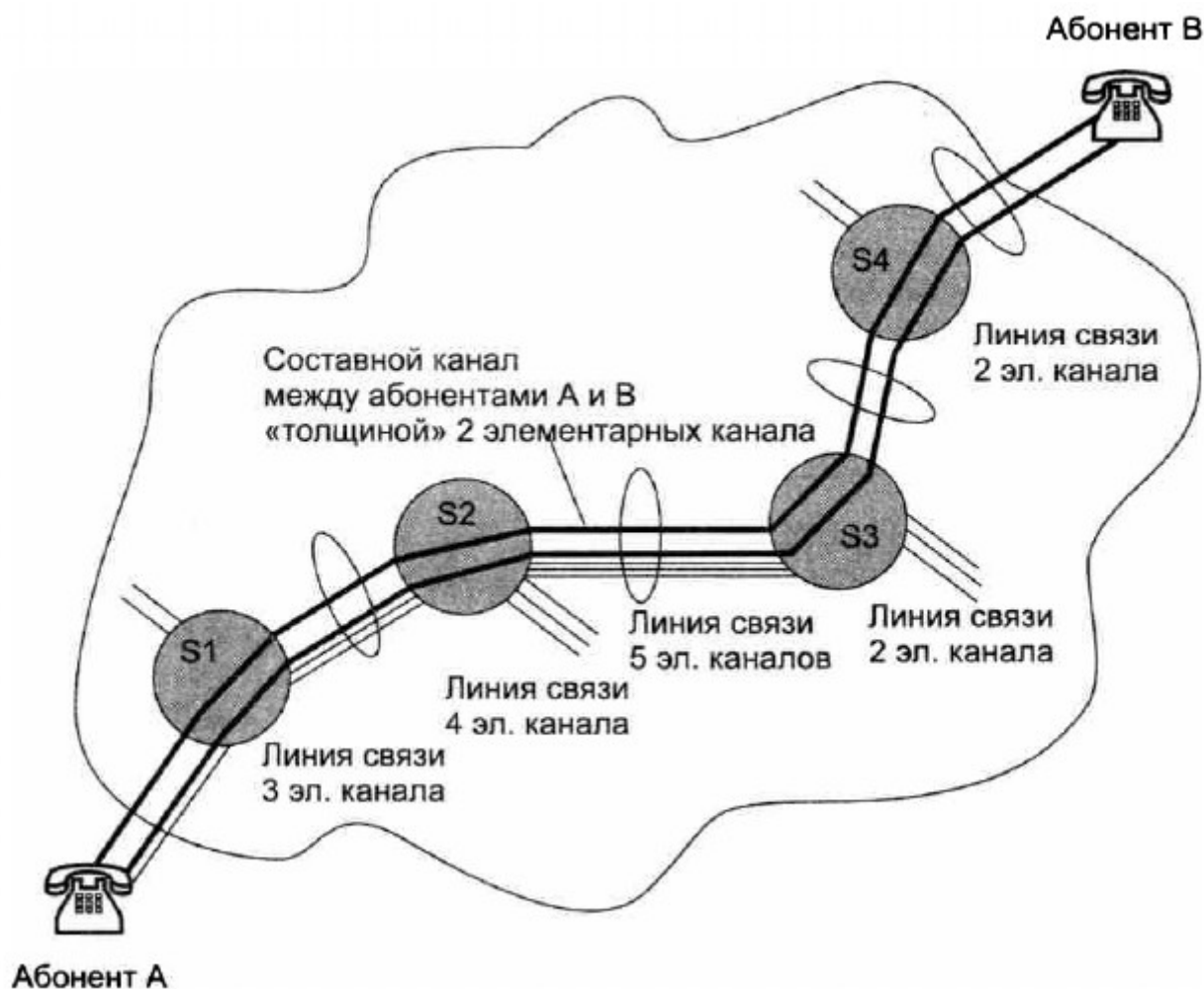
Исторически коммутация каналов появилась намного раньше коммутации пакетов и ведет свое происхождение от первых телефонных сетей.

Элементарный канал (или просто канал) — это базовая техническая характеристика сети с коммутацией каналов, представляющая собой некоторое фиксированное в пределах данного типа сетей значение пропускной способности.

Любая линия связи в сети с коммутацией каналов имеет пропускную способность, кратную элементарному каналу, принятому для данного типа сети.

Коммутация каналов и пакетов. Коммутация каналов

Особенностью сетей с коммутацией каналов является то, что пропускная способность каждой линии связи должна быть равна целому числу элементарных каналов.



Коммутация каналов и пакетов. Коммутация каналов

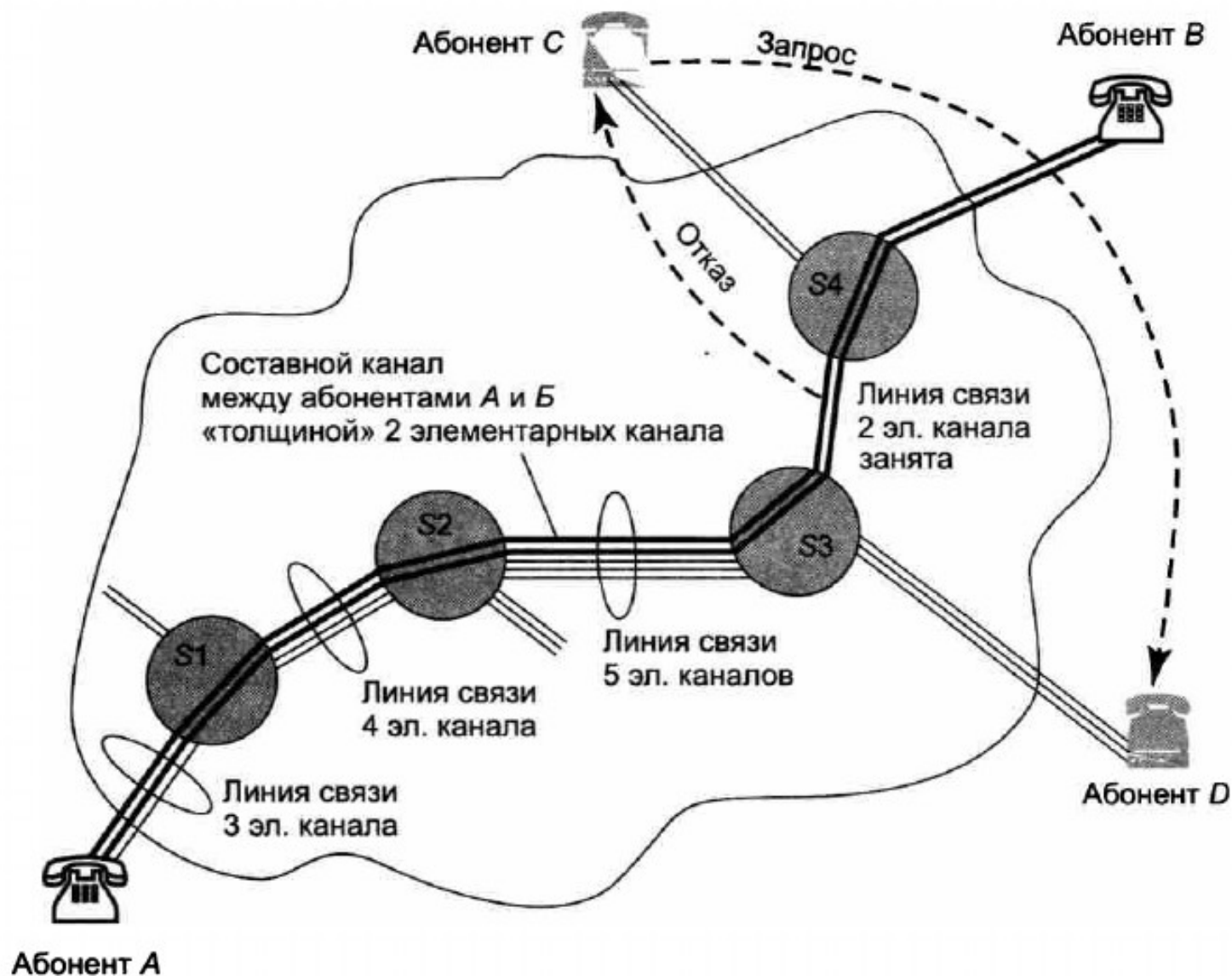


Рис. 3.3. Отказ в установлении соединения в сети с коммутацией каналов

Коммутация каналов и пакетов. Коммутация каналов

Сети с коммутацией каналов наиболее эффективно передают пользовательский трафик в том случае, когда скорость его постоянна в течение всего сеанса связи и максимально соответствует фиксированной пропускной способности физических линий связи сети.

Эффективность работы сети снижается, когда информационные потоки, генерируемые абонентами, приобретают пульсирующий характер.

Гораздо сильнее снижает эффективность сети с коммутацией каналов передача так называемого компьютерного трафика, то есть трафика, генерируемого приложениями, с которыми работает пользователь компьютера. Этот трафик практически всегда-является пульсирующим.

Коммутация каналов и пакетов. Коммутация пакетов

Важнейшим принципом функционирования сетей с коммутацией пакетов является представление информации, передаваемой по сети, в виде структурно отделенных друг от друга порций данных, называемых **пакетами**.

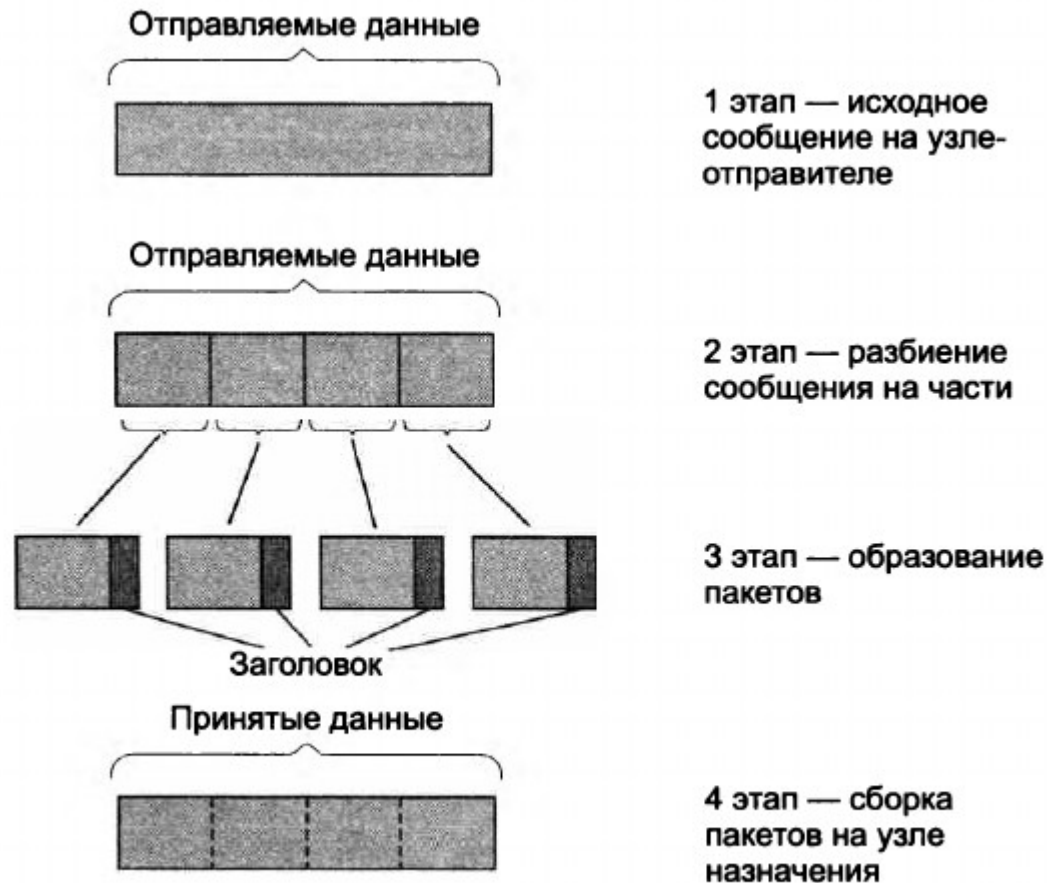


Рис. 3.5. Разбиение данных на пакеты

Коммутация каналов и пакетов. Коммутация пакетов

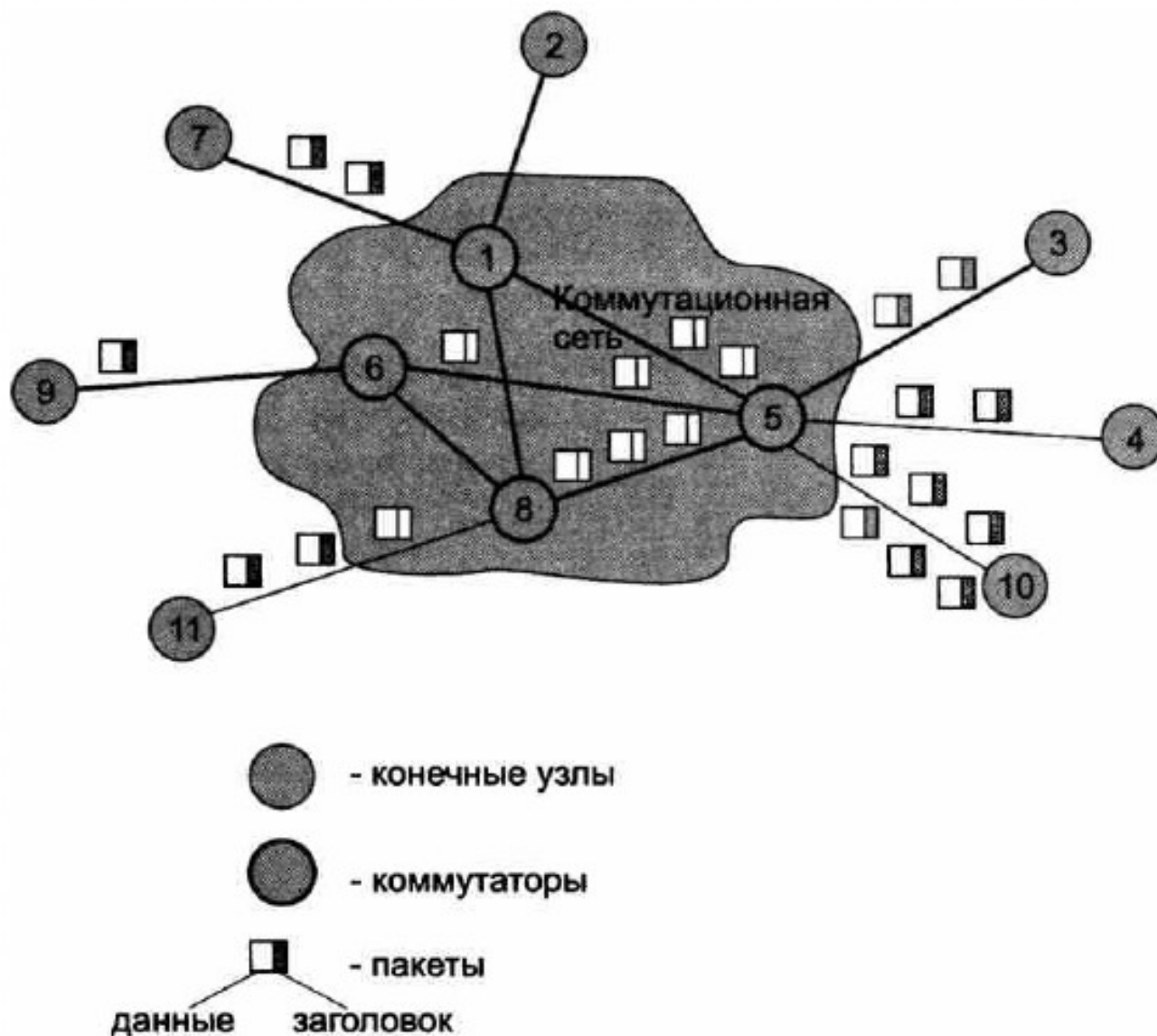


Рис. 3.6. Передача данных по сети в виде пакетов

Коммутация каналов и пакетов. Коммутация пакетов

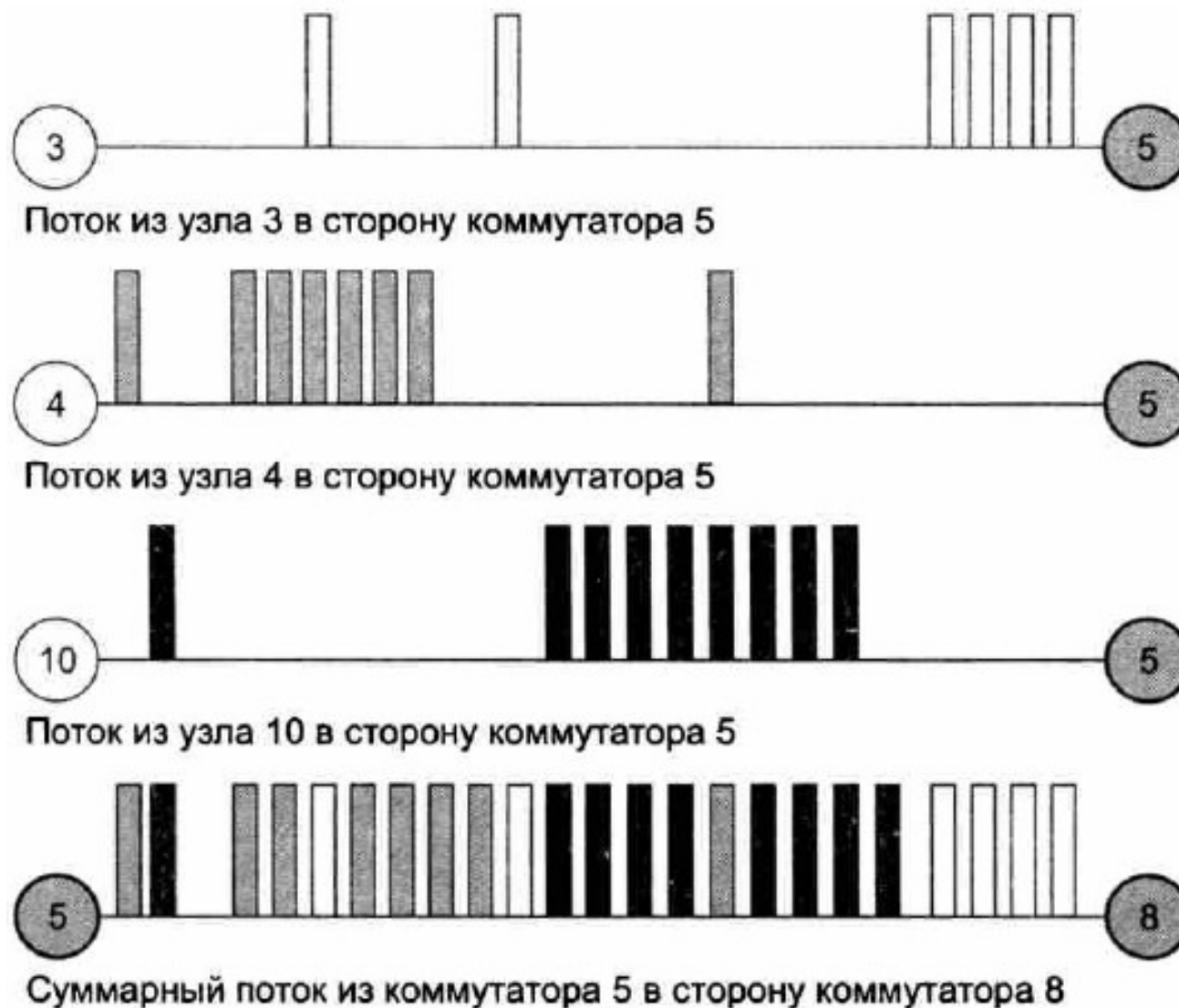


Рис. 3.7. Сглаживание трафика в сетях с коммутацией пакетов

Коммутация каналов и пакетов. Коммутация пакетов

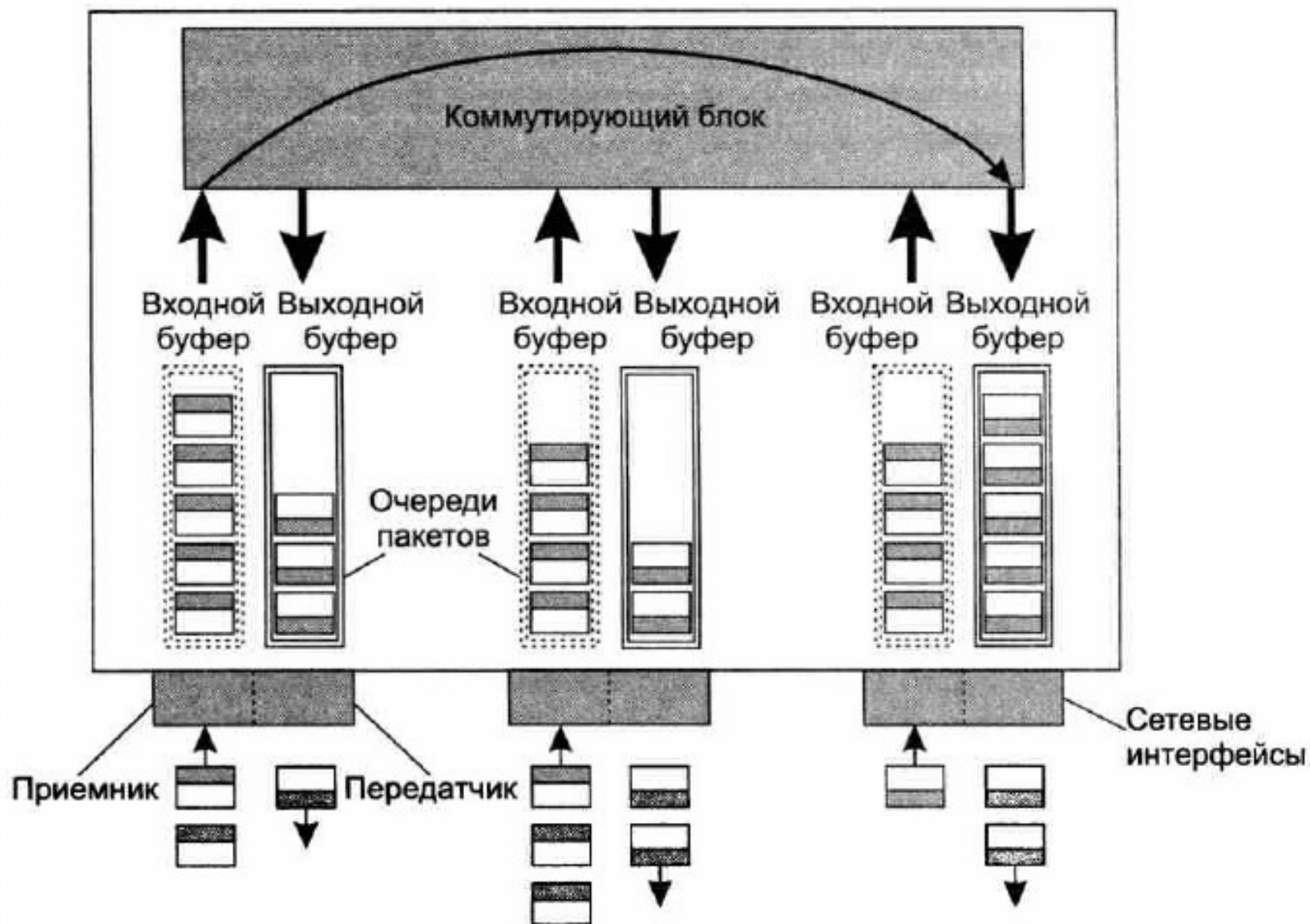


Рис. 3.8. Буферы и очереди пакетов в коммутаторе

Коммутация каналов и пакетов. Коммутация пакетов

Пакетный коммутатор может работать на основании одного из трех методов продвижения пакетов:

- Дейтаграммная передача;
- Передача с установлением логического соединения;
- Передача с установлением виртуального канала.

Коммутация пакетов. Дейтаграммная передача

Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты продвигаются (передаются от одного узла сети другому) независимо друг от друга на основании одних и тех же правил.

Коммутация пакетов. Дейтаграммная передача

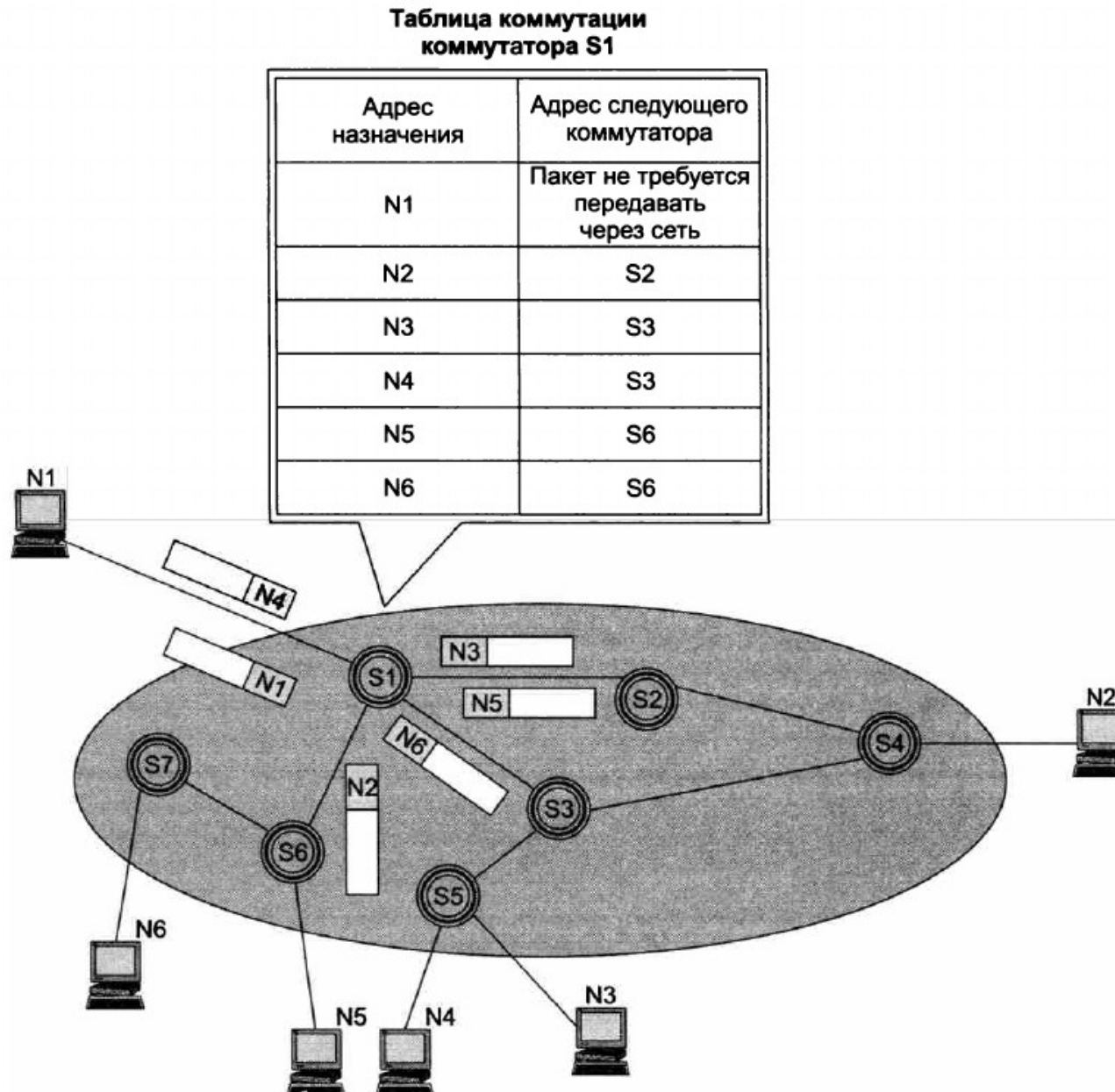


Рис. 3.9. Иллюстрация дейтаграммного принципа передачи пакетов

Коммутация пакетов. Логическое соединение

Процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена пакетами называется **установлением логического соединения**. Параметры, о которых договариваются два взаимодействующих узла, называются параметрами логического соединения.

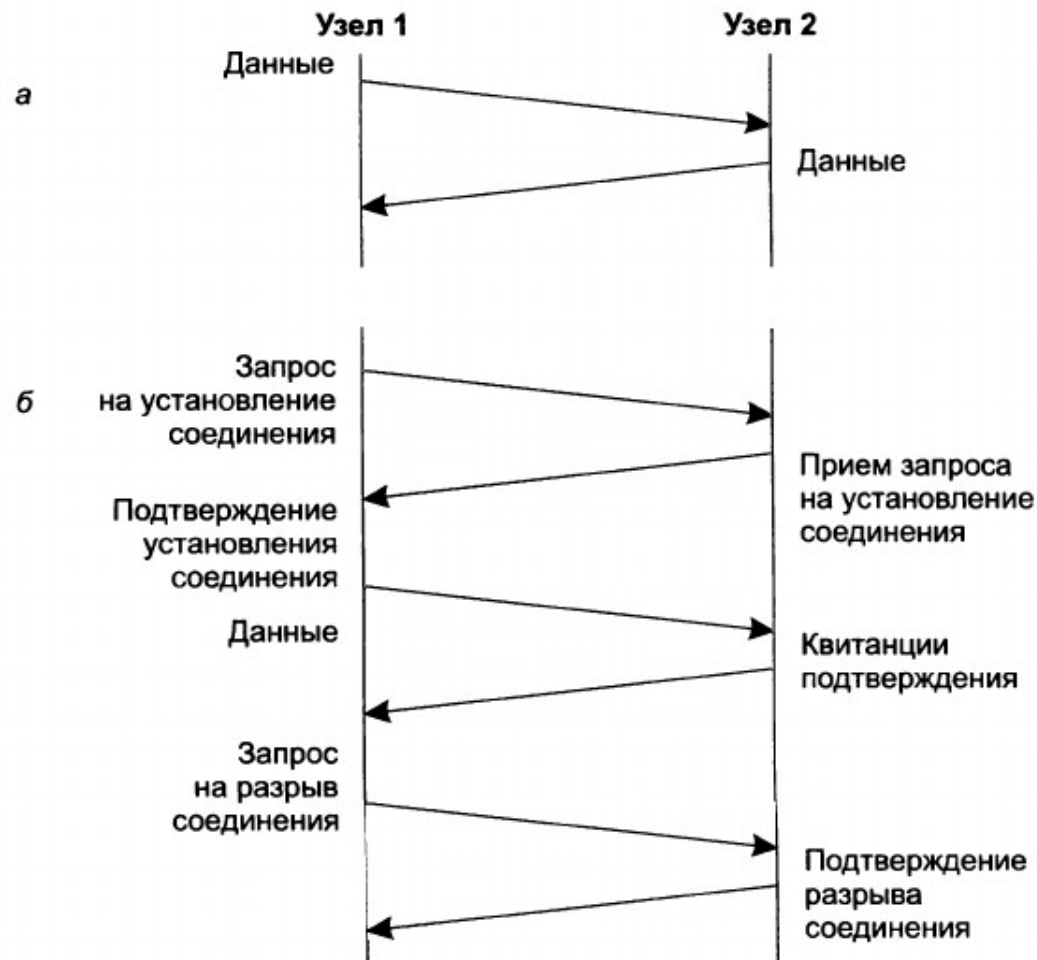


Рис. 3.10. Передача без установления соединения (а) и с установлением соединения (б)

Коммутация пакетов. Виртуальный канал

Единственный заранее проложенный фиксированный маршрут, соединяющий конечные узлы в сети с коммутацией пакетов, называют **виртуальным каналом** (virtual circuit, или virtual channel).

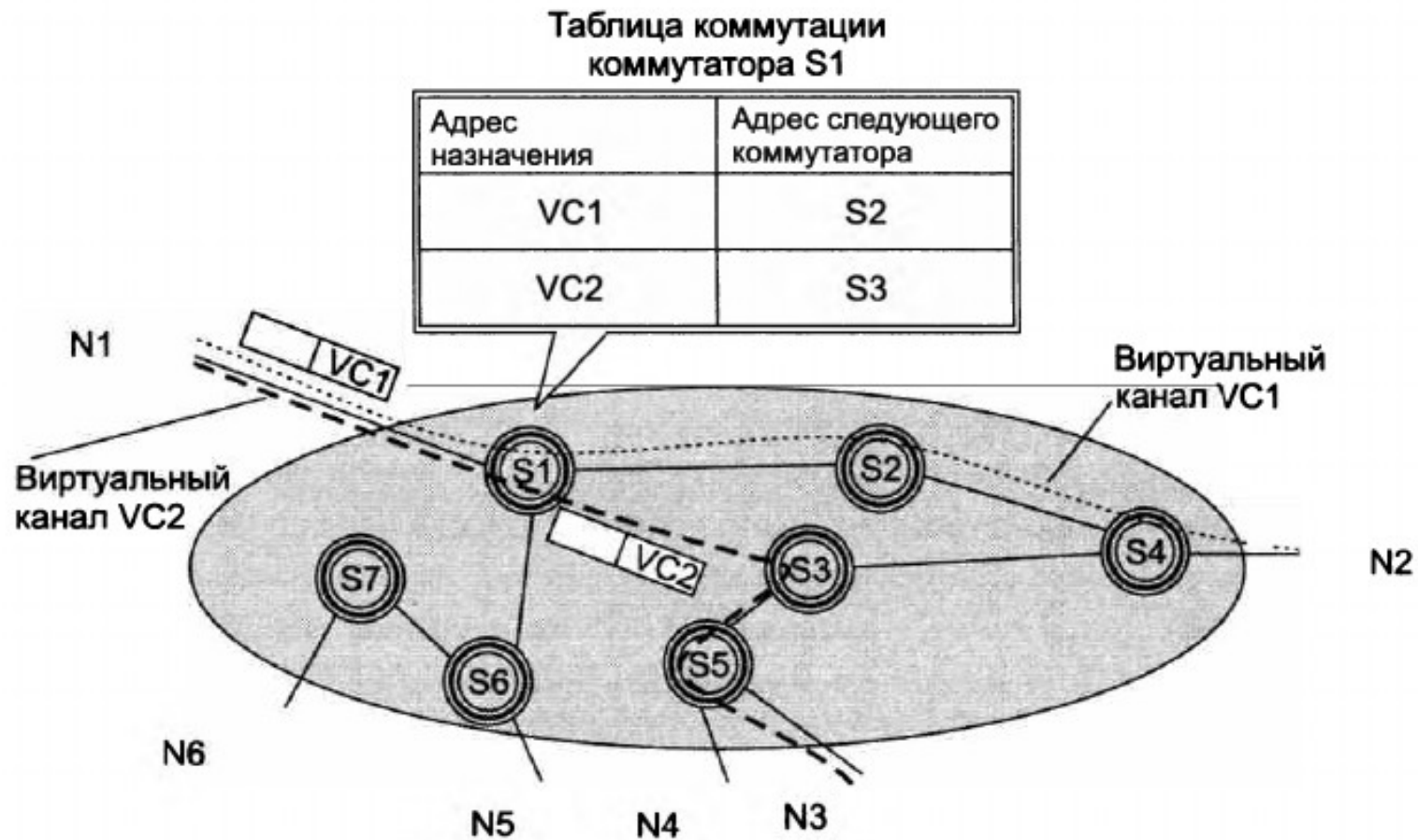


Рис. 3.11. Иллюстрация принципа работы виртуального канала

Ethernet — пример стандартной технологии с коммутацией пакетов

Рассмотрим, каким образом описанные ранее концепции воплощены в одной из первых стандартных сетевых технологий — технологии Ethernet, работающей с битовой скоростью 10 Мбит/с.

Топология. Существуют два варианта технологии Ethernet: Ethernet на разделяемой среде и коммутируемый вариант Ethernet. В первом случае все узлы сети разделяют общую среду передачи данных и сеть строится по топологии общей шины. На рис. 3.16 показан простейший вариант топологии — все компьютеры сети подключены к общей разделяемой среде, состоящей из одного сегмента коаксиального кабеля.

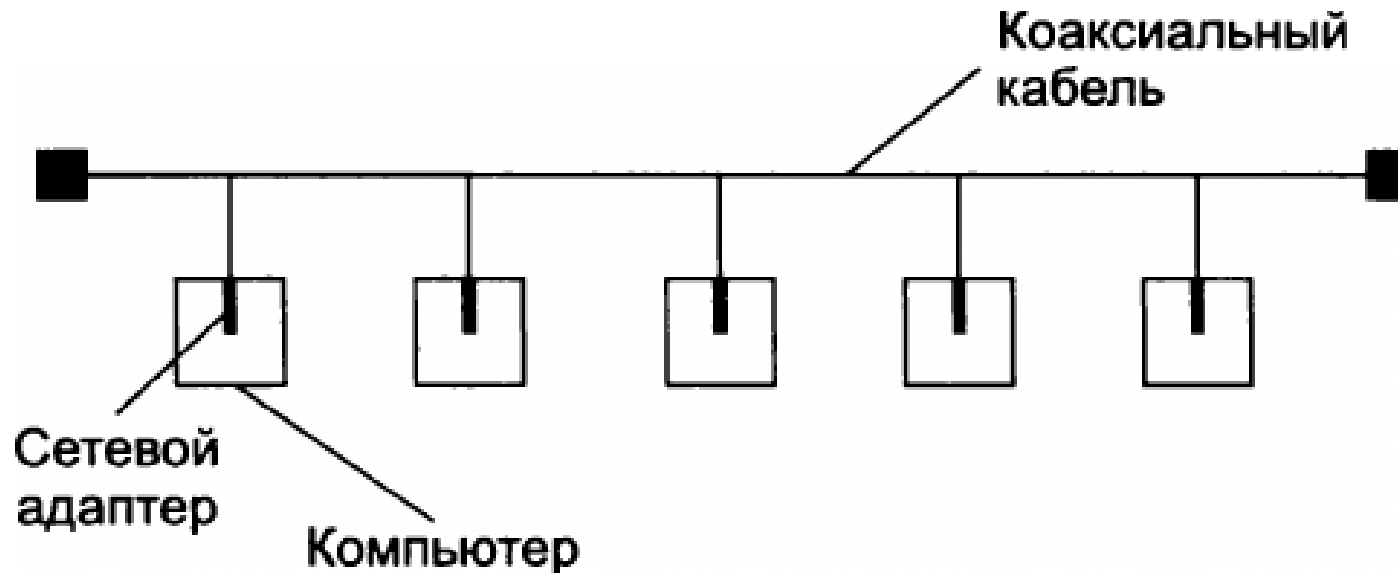


Рис. 3.16. Сеть Ethernet на разделяемой среде

Ethernet — пример стандартной технологии с коммутацией пакетов

Способ коммутации. В технологии Ethernet используется дейтаграммная коммутация пакетов. Единицы данных, которыми обмениваются компьютеры в сети Ethernet, называются кадрами. Кадр имеет фиксированный формат и наряду с полем данных содержит различную служебную информацию.

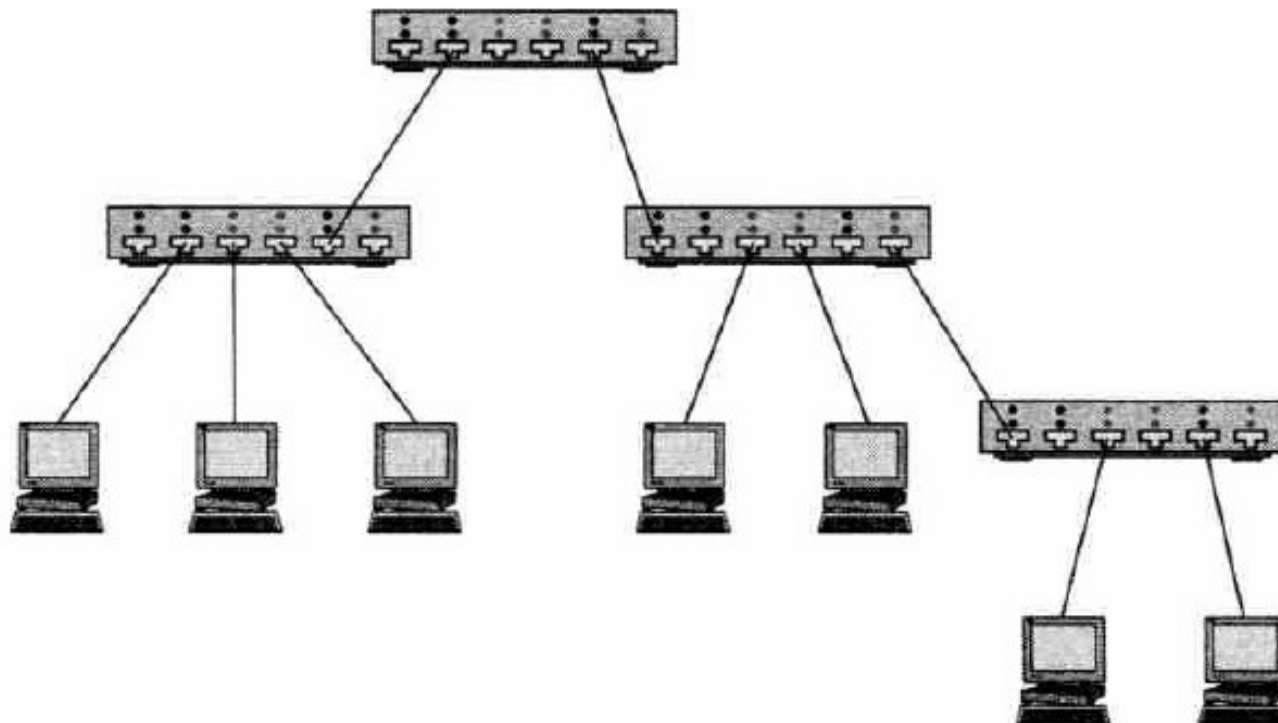


Рис. 3.17. Древоподобная топология коммутируемой сети Ethernet

Ethernet — пример стандартной технологии с коммутацией пакетов

Адресация. Каждый компьютер, а точнее каждый сетевой адаптер, имеет уникальный аппаратный адрес (так называемый MAC-адрес)

Разделение среды и мультиплексирование. В сети Ethernet на коммутаторах каждый канал является дуплексным каналом связи, и проблемы его разделения между интерфейсами узлов не возникает. Передатчики Ethernet-коммутаторов используют дуплексные каналы связи для мультиплексирования потоков кадров от разных конечных узлов.

Кодирование. Адаптеры в Ethernet работают с тактовой частотой 20 МГц, передавая в среду прямоугольные импульсы, соответствующие единицам и нулям данных компьютера. Когда начинается передача кадра, все его биты передаются в сеть с постоянной скоростью 10 М бит/с (каждый бит передается за два такта). Эта скорость определяется пропускной способностью линии связи в сети Ethernet.

Ethernet — пример стандартной технологии с коммутацией пакетов

Надежность. Для повышения надежности передачи данных в Ethernet используется стандартный прием — подсчет контрольной суммы и передача ее в концеvice кадра. Если принимающий адаптер путем повторного подсчета контрольной суммы обнаруживает ошибку в данных кадра, то такой кадр отбрасывается. Повторная передача кадра протоколом Ethernet не выполняется, эта задача должна решаться другими технологиями, например протоколом TCP в сетях TCP/IP.

Очереди. В коммутируемых сетях Ethernet очереди кадров, готовых к отправке, организуются обычным для сетей с коммутацией пакетов способом, то есть с помощью буферной памяти интерфейсов коммутатора.

Декомпозиция задачи сетевого взаимодействия. Многоуровневый подход

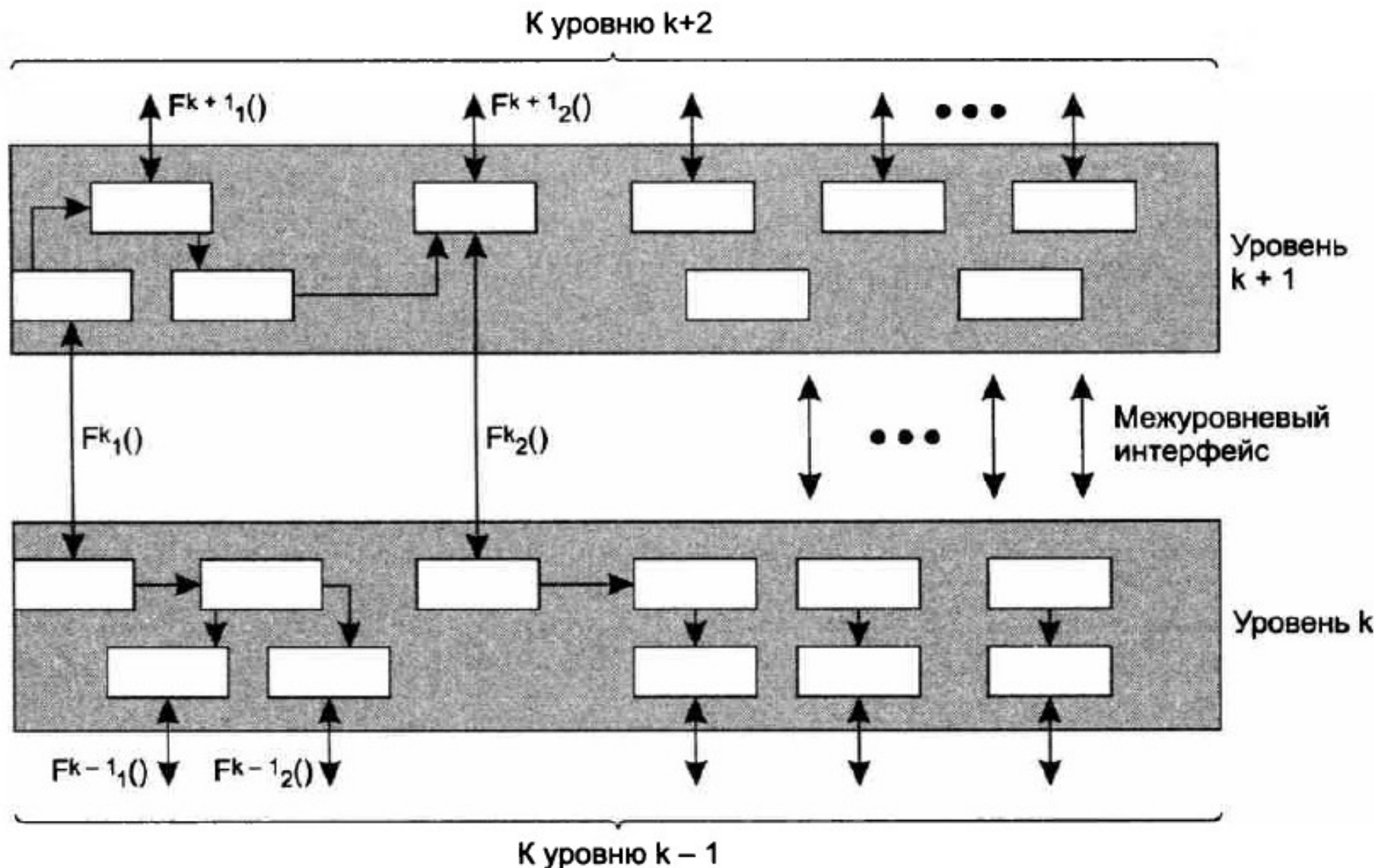


Рис. 4.3. Концепция многоуровневого взаимодействия

Протокол и стек протоколов

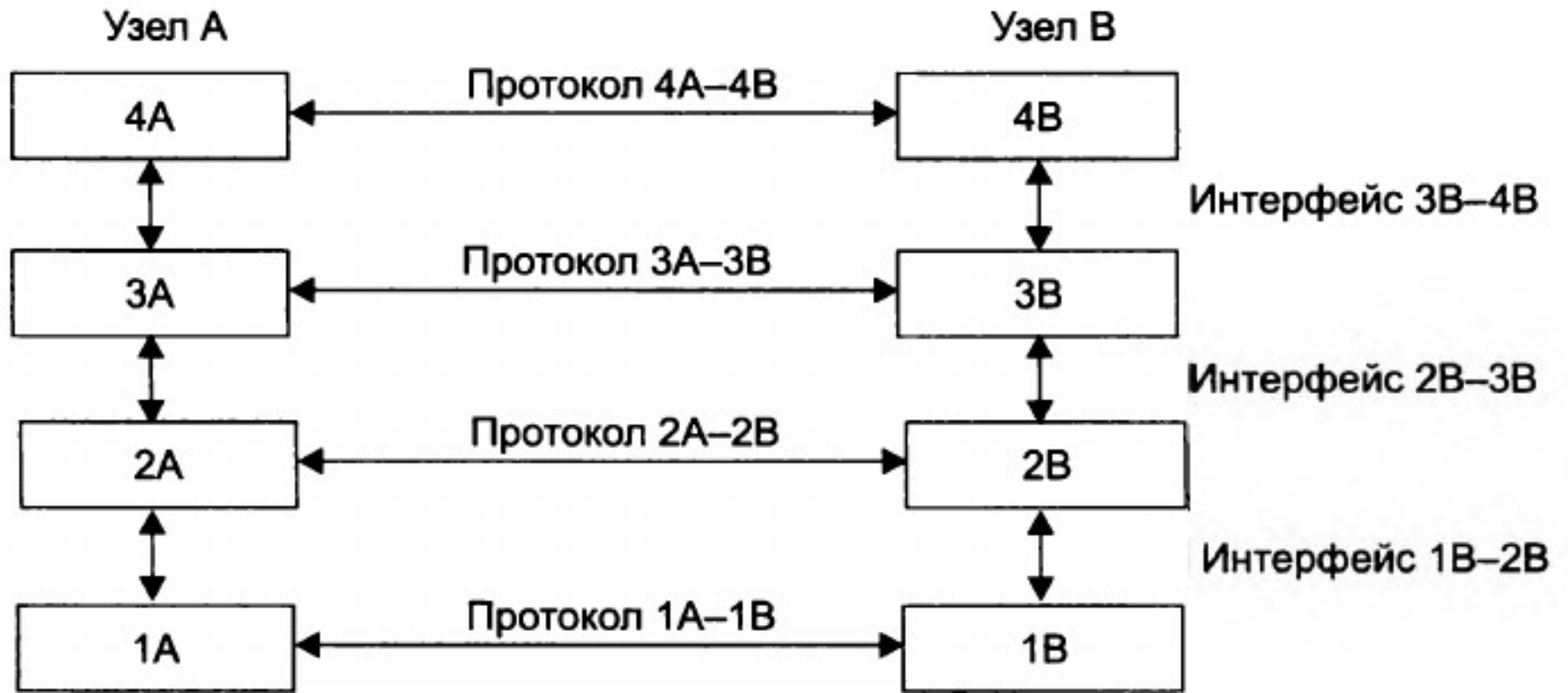


Рис. 4.5. Взаимодействие двух узлов

Модель OSI

К концу 70-х годов в мире уже существовало большое количество фирменных стеков коммуникационных протоколов, среди которых можно назвать, например, такие популярные стеки, как DECnet, TCP/IP и IBM SNA. Подобное разнообразие средств межсетевого взаимодействия вывело на первый план проблему несовместимости устройств, использующих разные протоколы.

В начале 80-х годов ряд международных организаций по стандартизации, в частности **International Organization for Standardization (ISO)**, часто называемая International Standards Organization, а также International Telecommunications Union (ITU) и некоторые другие, разработали стандартную модель взаимодействия открытых систем (**Open System Interconnection, OSI**). Эта модель сыграла значительную роль в развитии компьютерных сетей.

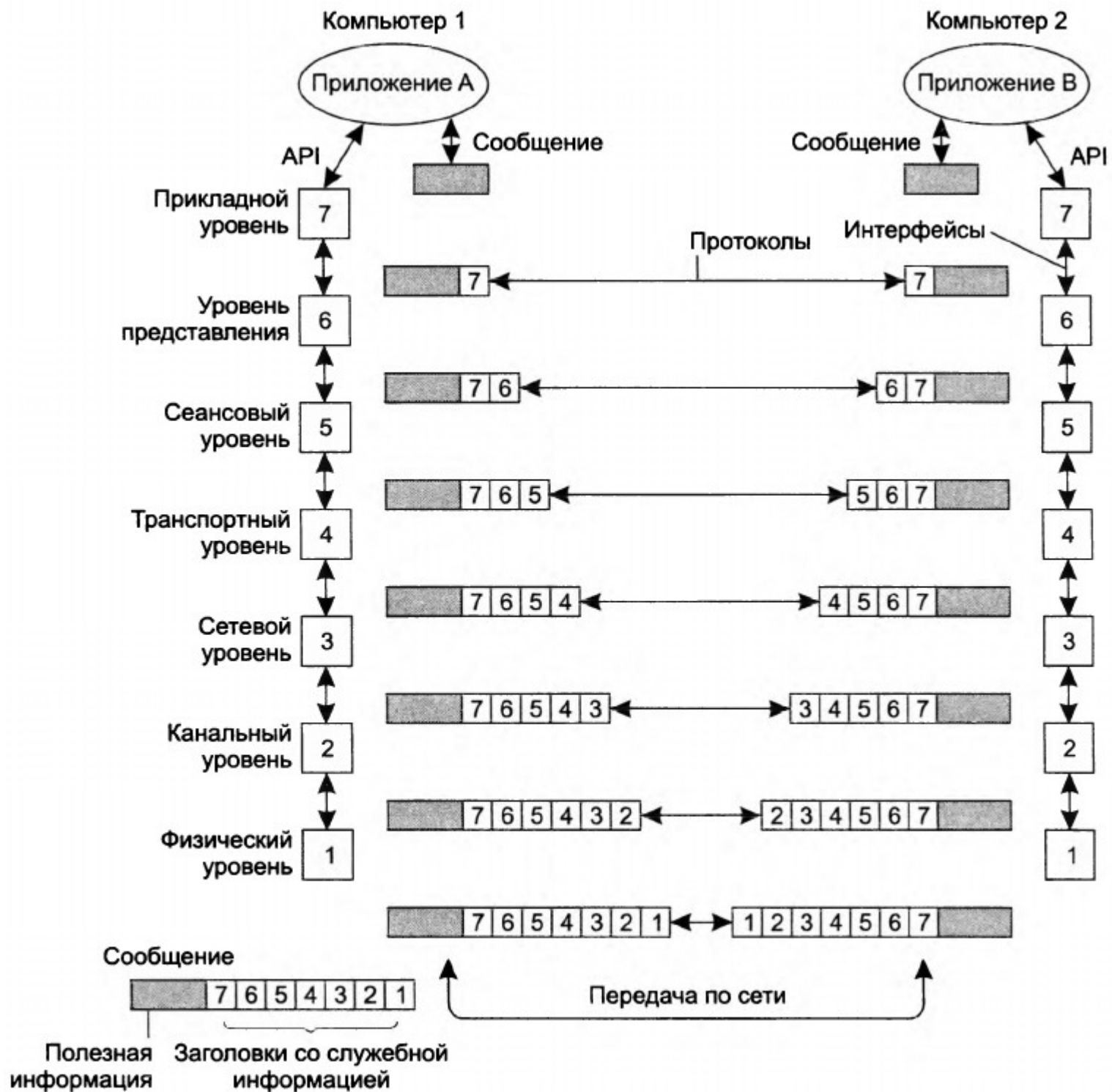


Рис. 4.6. Модель взаимодействия открытых систем ISO/OSI

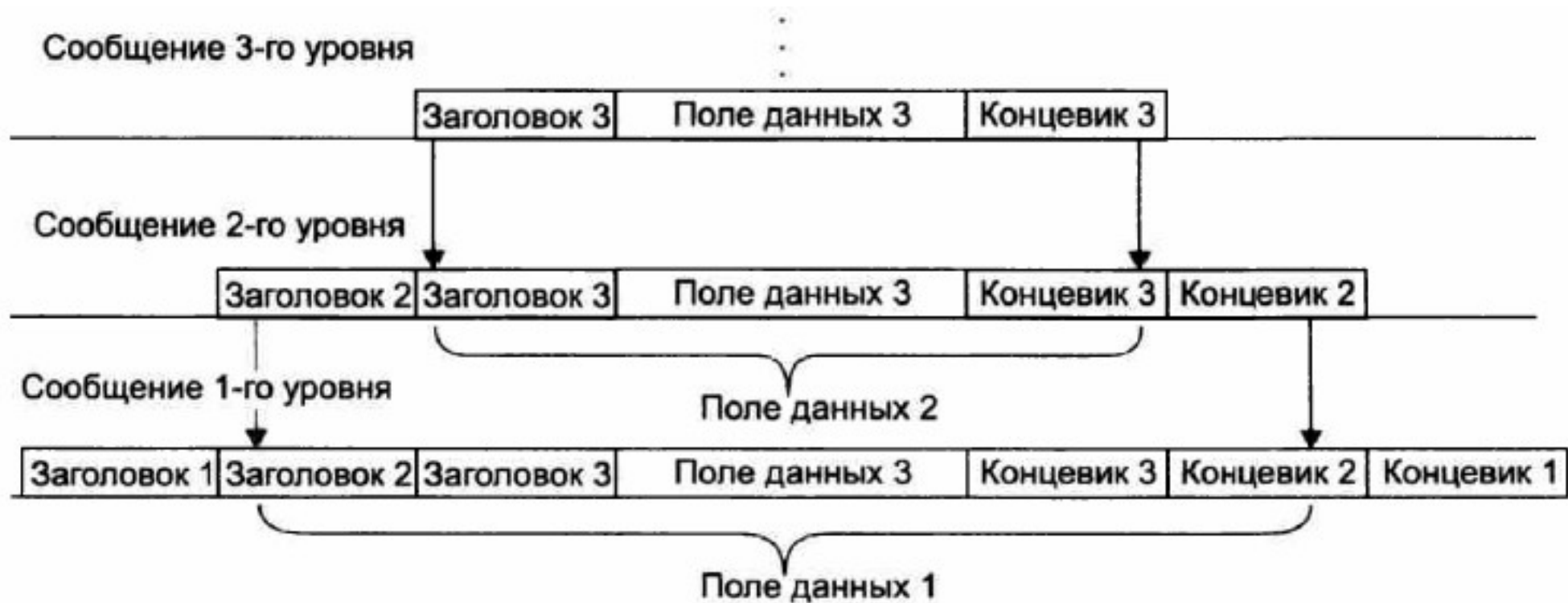


Рис. 4.7. Вложенность сообщений различных уровней

1. Физический уровень

Физический уровень (physical layer) имеет дело с передачей потока битов по физическим каналам связи, таким как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Примером протокола физического уровня может служить спецификация **1000Base-T** технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную витую пару категории 5 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100 метров, манчестерский код для представления данных в кабеле, а также некоторые другие характеристики среды и электрических сигналов.

Физический уровень не вникает в смысл информации, которую он передает.

2. Канальный уровень

Канальный уровень (data link layer) обеспечивает прозрачность соединения для сетевого уровня. Для этого он предлагает ему следующие услуги:

- установление логического соединения между взаимодействующими узлами;
- согласование в рамках соединения скоростей передатчика и приемника информации;
- обеспечение надежной передачи, обнаружение и коррекция ошибок.

Для решения этих задач канальный уровень формирует из пакетов собственные протокольные единицы данных — **кадры**, состоящие из поля данных и заголовка. Канальный уровень помещает пакет в поле данных одного или нескольких кадров и заполняет собственной служебной информацией заголовки кадров.

3. Сетевой уровень

Сетевой уровень (network layer) служит для образования единой транспортной системы, объединяющей несколько сетей и называемой составной сетью, или интернетом.

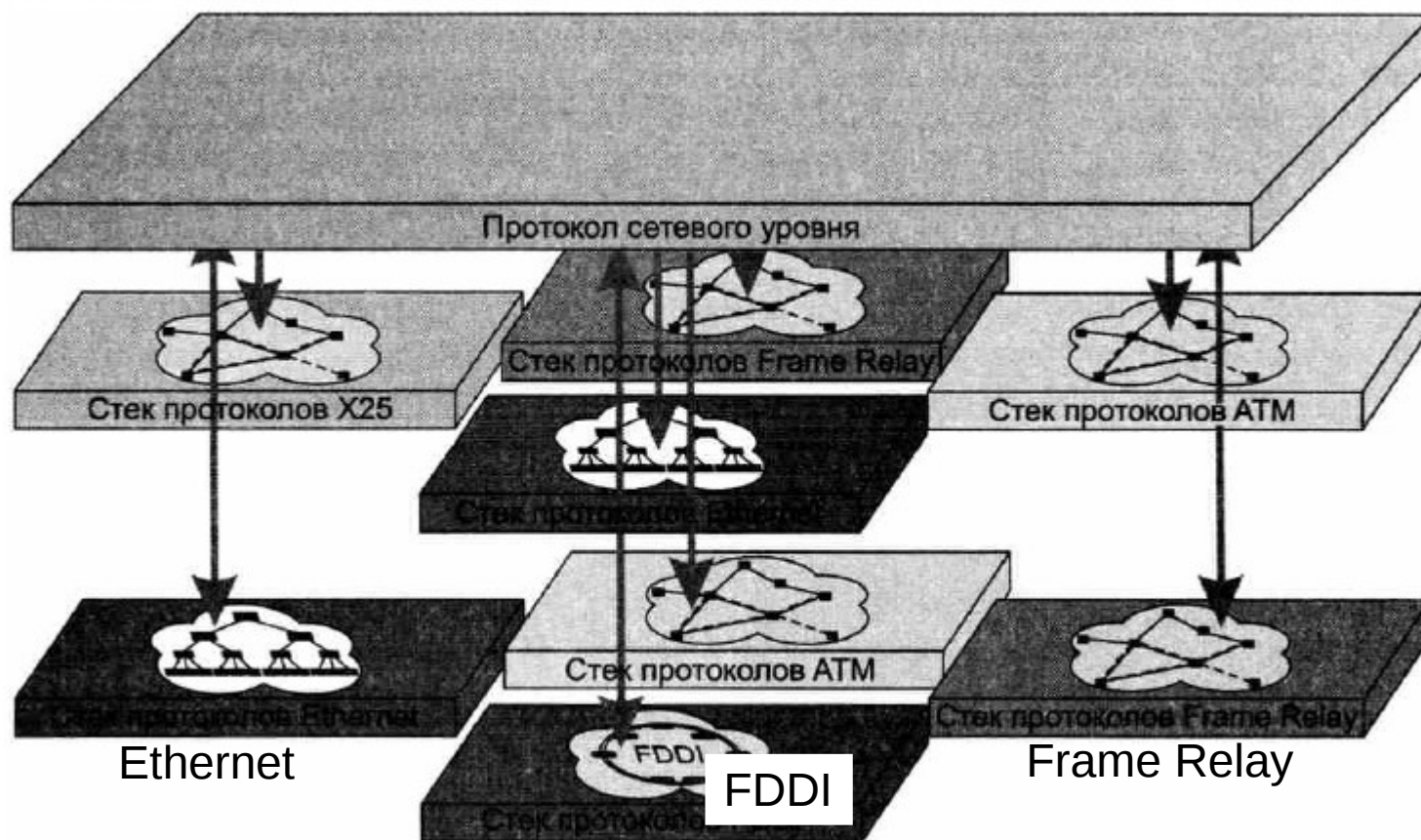


Рис. 4.8. Иллюстрация необходимости сетевого уровня

3. Сетевой уровень

Можно найти аналогию между функционированием сетевого уровня и международной почтовой службы, такой, например, как DHL или TNT. Представим, что некоторый груз необходимо доставить из города Абра в город Кадабра, причем эти города расположены на разных континентах. Для доставки груза международная почта использует услуги различных региональных перевозчиков:

- железную дорогу; морской транспорт; авиаперевозчиков; автомобильный транспорт.

Эти перевозчики могут рассматриваться как аналоги сетей канального уровня, причем каждая «сеть» здесь построена на основе собственной технологии. Из этих региональных служб международная почтовая служба должна организовать единую слаженно работающую сеть. Для этого международная почтовая служба должна, во-первых, продумать маршрут перемещения почты, во-вторых, координировать работу в пунктах смены перевозчиков (например, выгружать почту из вагонов и размещать ее в транспортных отсеках самолетов). Каждый же перевозчик ответствен только за перемещение почты по своей части пути и не несет никакой ответственности за состояние почты за его пределами.

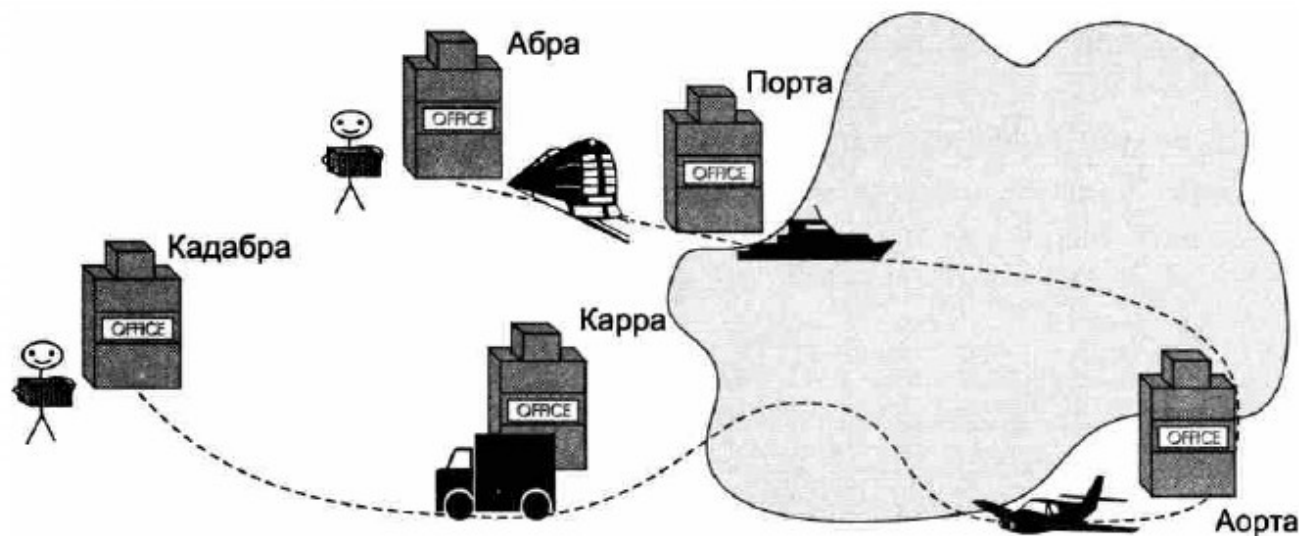


Рис. 4.10. Работа международной почтовой службы

3. Сетевой уровень

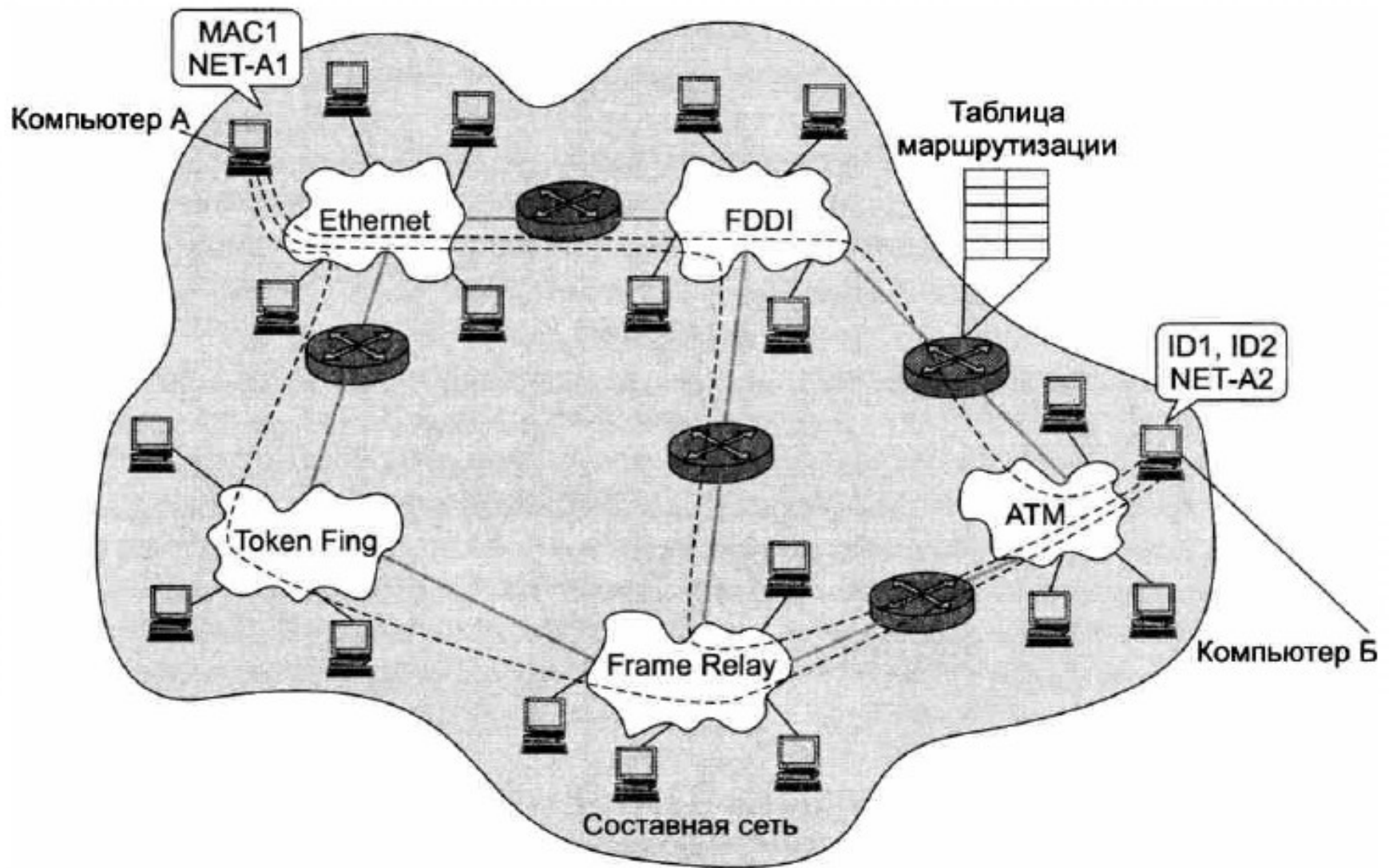


Рис. 4.9. Пример составной сети

4. Транспортный уровень

Транспортный уровень (transport layer) обеспечивает приложениям и верхним уровням стека — прикладному, представления и сеансовому — передачу данных с той степенью надежности, которая им требуется.

Модель OSI определяет пять классов транспортного сервиса: от низшего класса 0 до высшего класса 4.

Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное — способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети — компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы **TCP** и **UDP** стека **TCP/IP** и протокол **SPX** стека **Novell**.

Протоколы нижних четырех уровней обобщенно называют **сетевым транспортом**, или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Оставшиеся три верхних уровня решают задачи предоставления прикладных сервисов, используя нижележащую транспортную подсистему.

5. Сеансовый уровень

Сеансовый уровень (session layer) управляет взаимодействием сторон: фиксирует, какая из сторон является активной в настоящий момент, и предоставляет средства синхронизации сеанса.

Эти средства позволяют в ходе длинных передач сохранять информацию о состоянии этих передач в виде контрольных точек, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала.

На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов. Функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

6. Уровень представления

Уровень представления (presentation layer), как явствует из его названия, обеспечивает представление передаваемой по сети информации, не меняя при этом ее содержания.

За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и EBCDIC.

На этом уровне могут выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных служб.

Примером такого протокола является протокол SSL (Secure Socket Layer — слой защищенных сокетов), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

7. Прикладной уровень

Прикладной уровень (application layer) —это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к общим ресурсам, таким как файлы, принтеры или гипертекстовые веб-страницы, а также организуют свою совместную работу, например по протоколу электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением.

Существует очень большое разнообразие протоколов и соответствующих служб прикладного уровня. Приведем в качестве примера несколько наиболее распространенных протоколов этого уровня:

- протоколы доступа к файлам NFS и FTP в стеке TCP/IP, SMB в Microsoft Windows, NCP в операционной системе Novell NetWare;
- почтовые протоколы SMTP, IMAP, POP3;
- протокол передачи гипертекстовых сообщений HTTP.

Модель OSI и сети с коммутацией каналов

Как уже было упомянуто, модель OSI описывает процесс взаимодействия устройств в сети с **коммутацией пакетов**. А как же обстоит дело с сетями **коммутации каналов**?

Общей справочной модели, подобной модели OSI, для сетей с коммутацией каналов **не существует**. Например, различные типы телефонных сетей имеют собственные стеки протоколов, отличающиеся количеством уровней и распределением функций между уровнями.

Источники стандартов

- **стандарты отдельных фирм**, например стек протоколов SNA компании IBM или графический интерфейс OPEN LOOK для Unix-систем компании Sun;
- **стандарты специальных комитетов и объединений** создаются несколькими компаниями, например стандарты технологии ATM, разрабатываемые специально созданным объединением ATM Forum, которое насчитывает около 100 коллективных участников, или стандарты союза Fast Ethernet Alliance, касающиеся технологии 100 Мбит Ethernet;
- **национальные стандарты**, например стандарт FDDI, представляющий один из многочисленных стандартов института ANSI, или стандарты безопасности для операционных систем, разработанные центром NCSC министерства обороны США;
- **международные стандарты**, например модель и стек коммуникационных протоколов Международной организации по стандартизации (ISO), многочисленные стандарты Международного союза электросвязи (ITU), в том числе стандарты на сети с коммутацией пакетов X.25, сети Frame Relay, ISDN, модемы и многие другие.



Уровни
модели
OSI

Рис. 4.11. Стек протоколов OSI

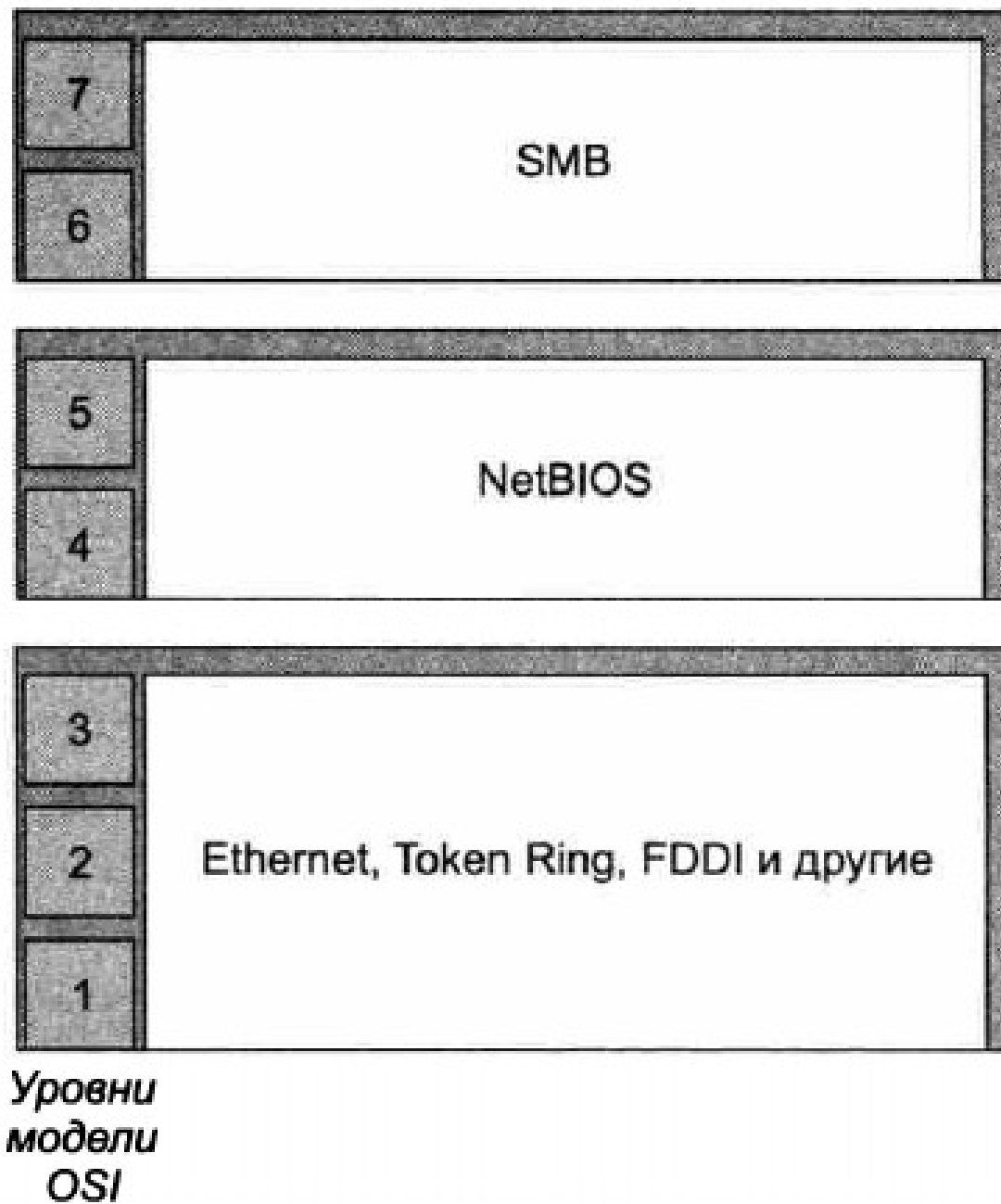


Рис. 4.12. Стек NetBIOS/SMB

Модель OSI	IBM/Microsoft		TCP/IP		Novell		Стек OSI
Прикладной		SMB		Telnet, FTP, SNMP, SMTP, WWW		NCP, SAP	X.400, X.500, FTAM
Представления							Протокол уровня представления OSI
Сеансовый							Сеансовый протокол OSI
Транспортный		NetBIOS		TCP		SPX	Транспортный протокол OSI
Сетевой			IP, RIP, OSPF				IPX, RIP, NLSP
Канальный		802.3 (Ethernet), 802.5 (Token Ring), FDDI, ATM, PPP					
Физический		Коаксиал, экранированная и неэкранированная витая пара, оптоволокно, радиоволны					

Рис. 4.13. Соответствие популярных стеков протоколов модели OSI

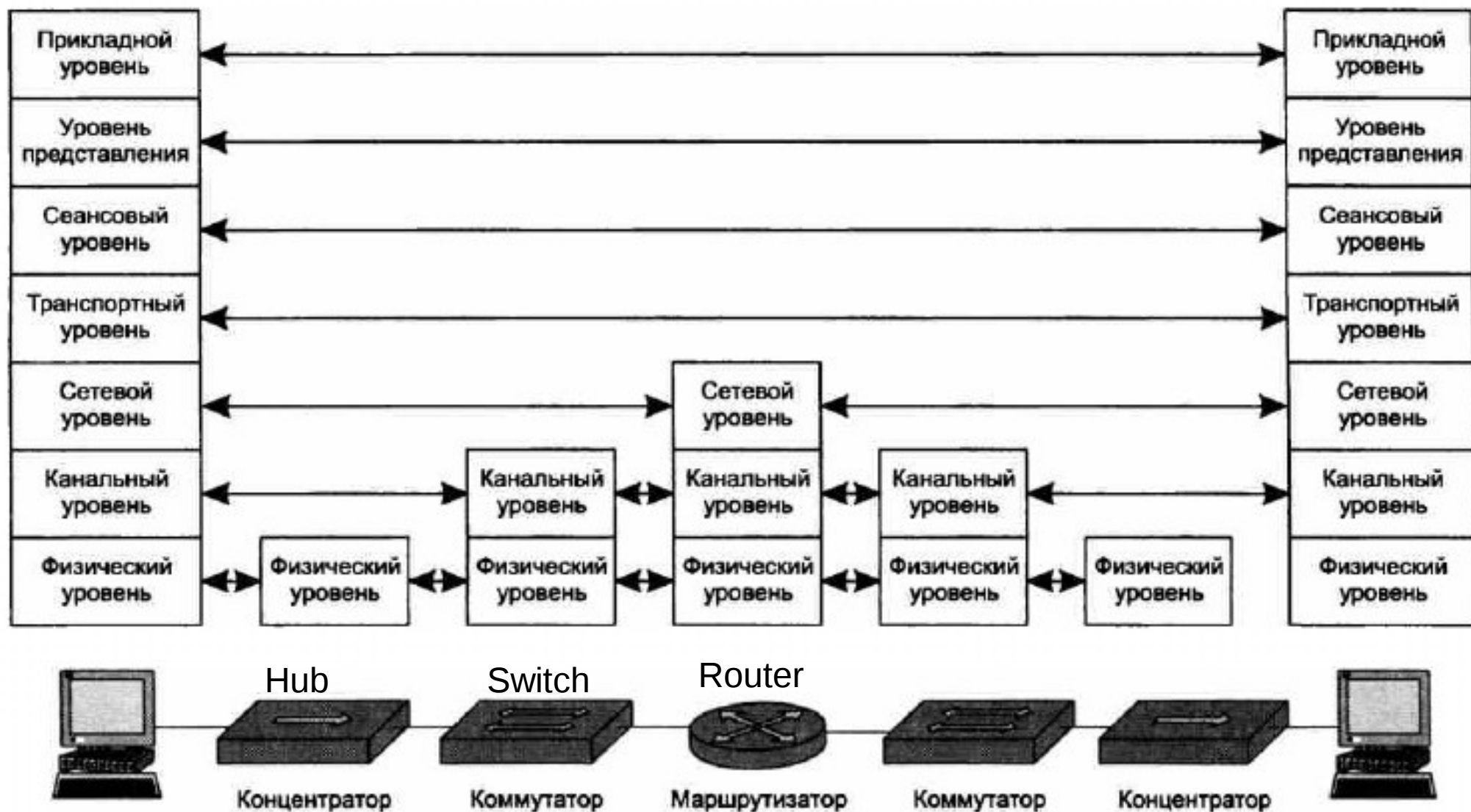


Рис. 4.14. Соответствие функций различных устройств сети уровням модели OSI

Виртуальные локальные сети

Виртуальной локальной сетью (Virtual Local Area Network, VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети.

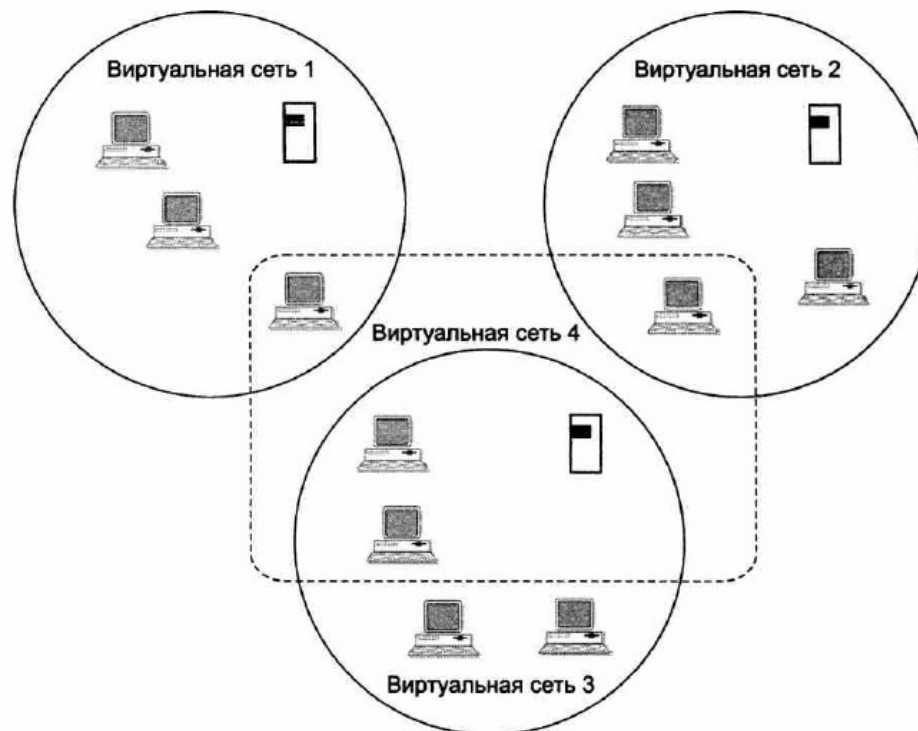


Рис. 13.5. Виртуальные локальные сети

Виртуальные локальные сети

Достоинством технологии виртуальных сетей является то, что она позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры.

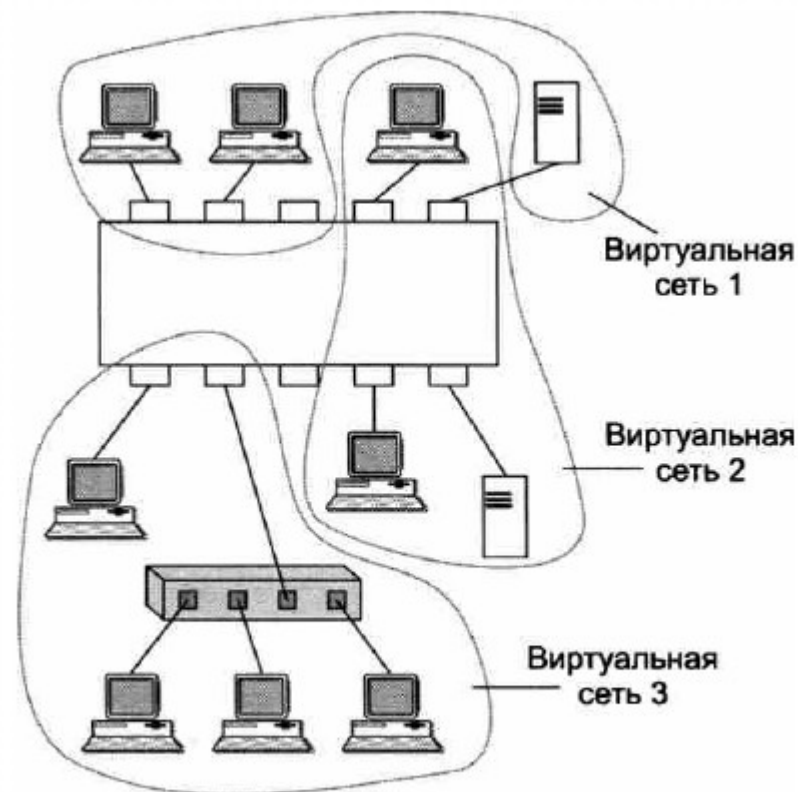


Рис. 13.7. Виртуальные сети, построенные на одном коммутаторе

Альтернативные маршруты в виртуальных локальных сетях

Чтобы в сети можно было использовать разные покрывающие деревья для разных виртуальных локальных сетей, существует специальная версия протокола, называемая множественным протоколом покрывающего дерева (Multiple Spanning Tree Protocol, MSTP).

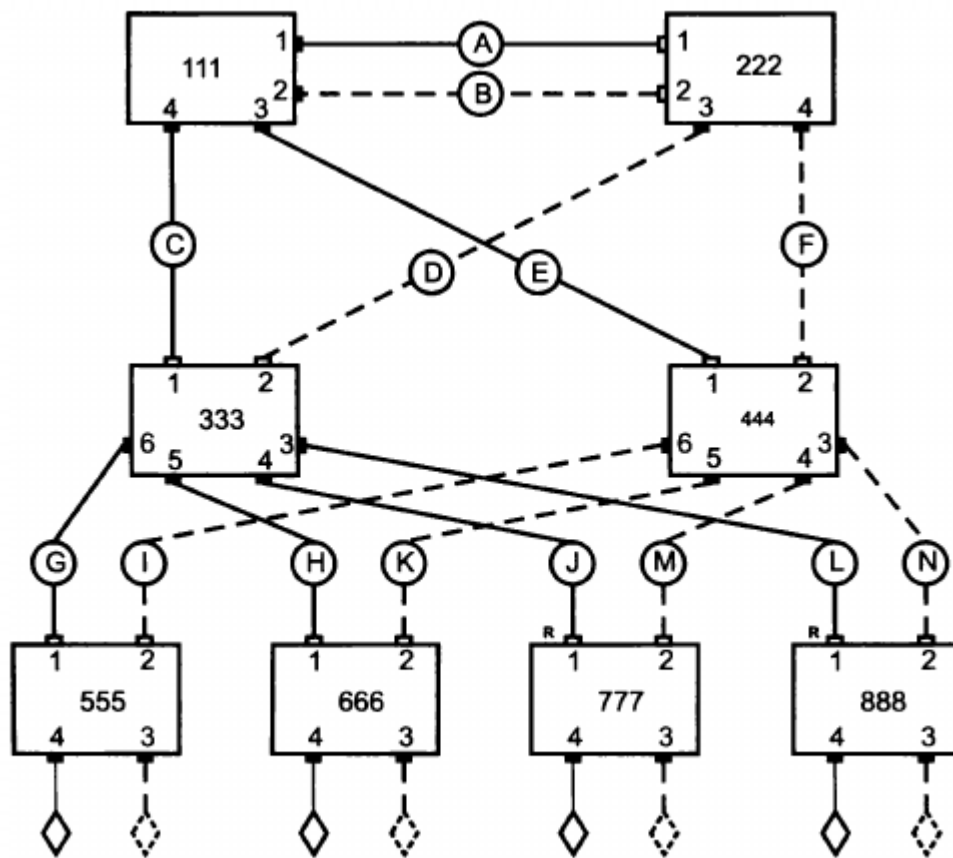


Рис. 13.11. Два покрывающих дерева, построенные по протоколу MSTP

Адресация в стеке протоколов TCP/IP

Важную часть технологии TCP/IP составляют задачи адресации, к числу которых относятся следующие:

- Согласованное использование адресов различного типа. Эта задача включает отображение адресов разных типов друг на друга, например сетевого IP-адреса на локальный, доменного имени — на IP-адрес.
- Обеспечение уникальности адресов. В зависимости от типа адреса требуется обеспечивать однозначность адресации в пределах компьютера, подсети, корпоративной сети или Интернета.
- Конфигурирование сетевых интерфейсов и сетевых приложений.

Адресация в стеке протоколов TCP/IP

Сегодня стек TCP/IP широко используется как в глобальных, так и в локальных сетях. Этот стек имеет иерархическую структуру, в которой определено четыре уровня (рис. 14.1).

Прикладной уровень	FTP, Telnet, HTTP, SMTP, SNMP, TFTP
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, ICMP, RIP, OSPF
Уровень сетевых интерфейсов	Не регламентируется

Рис. 14.1. Иерархическая структура стека TCP/IP

Адресация в стеке протоколов TCP/IP

Прикладной уровень стека TCP/IP соответствует трем верхним уровням модели OSI: прикладному, представления и сеансовому.

Он объединяет сервисы, предоставляемые системой пользовательским приложениям. За долгие годы применения в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и служб прикладного уровня. К ним относятся такие распространенные протоколы, как протокол передачи файлов (File Transfer Protocol, FTP), протокол эмуляции терминала telnet, простой протокол передачи почты (Simple Mail Transfer Protocol, SMTP), протокол передачи гипертекста (Hypertext Transfer Protocol, HTTP) и многие другие. Протоколы прикладного уровня развертываются на хостах.

Транспортный уровень стека TCP/IP может предоставлять вышележащему уровню два типа сервиса:

- гарантированную доставку обеспечивает протокол управления передачей (Transmission Control Protocol, TCP);
- доставку по возможности, или с максимальными усилиями, обеспечивает протокол пользовательских дейтаграмм (User Datagram Protocol, UDP).

Адресация в стеке протоколов TCP/IP

Сетевой уровень, называемый также уровнем интернета, является стержнем всей архитектуры TCP/IP. Именно этот уровень, функции которого соответствуют сетевому уровню модели OSI, обеспечивает перемещение пакетов в пределах составной сети, образованной объединением нескольких подсетей. Протоколы сетевого уровня поддерживают интерфейс с вышележащим транспортным уровнем, получая от него запросы на передачу данных по составной сети, а также с нижележащим уровнем сетевых интерфейсов.

Уровень сетевых интерфейсов. Нижние уровни модели OSI (канальный и физический) реализуют множество функций: доступа к среде передачи, формирования кадров, согласования величин электрических сигналов, кодирования и синхронизации, а также некоторые другие. Все эти весьма конкретные функции составляют суть таких протоколов обмена данными, как Ethernet, PPP и многих других.

У нижнего уровня стека TCP/IP задача существенно проще — он отвечает только за организацию взаимодействия с подсетями разных технологий, входящими в составную сеть.

TCP/IP рассматривает любую подсеть, входящую в составную сеть, как средство транспортировки пакетов между двумя соседними маршрутизаторами.

Задачу организации интерфейса между технологией TCP/IP и любой другой технологией промежуточной сети упрощенно можно свести к двум задачам:

- упаковка (инкапсуляция) IP-пакета в единицу передаваемых данных промежуточной сети;
- преобразование сетевых адресов в адреса технологии данной промежуточной сети.

Типы адресов стека TCP/IP

Для идентификации сетевых интерфейсов используются три типа адресов:

- локальные (аппаратные) адреса;
- сетевые адреса (IP-адреса);
- символьные (доменные) имена.

Локальные адреса

В большинстве технологий LAN (Ethernet, FDDI, Token Ring) для однозначной адресации интерфейсов используются MAC-адреса. Существует немало технологий (X.25, ATM, frame relay), в которых применяются другие схемы адресации. Роль, которую играют эти адреса в TCP/IP, не зависит от того, какая именно технология используется в подсети, поэтому все они имеют общее название — **локальные (аппаратные) адреса**.

Сетевые IP-адреса

Чтобы технология TCP/IP могла решать свою задачу объединения сетей, ей необходима собственная глобальная система адресации, не зависящая от способов адресации узлов в отдельных сетях.

Эта система адресации должна позволять универсальным и однозначным способом идентифицировать любой интерфейс составной сети.

Очевидным решением является уникальная нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей. Пара, состоящая из **номера сети** и **номера узла**, отвечает поставленным условиям и может являться **сетевым адресом**, или в терминологии TCP/IP — IP-адресом.

Доменные имена

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса. Например, команда `ftp://192.45.66.17` будет устанавливать сеанс связи с нужным ftp-сервером, а команда `http://203.23.106.33` откроет начальную страницу на корпоративном веб-сервере. Однако пользователи обычно предпочитают работать с более удобными символьными именами компьютеров.

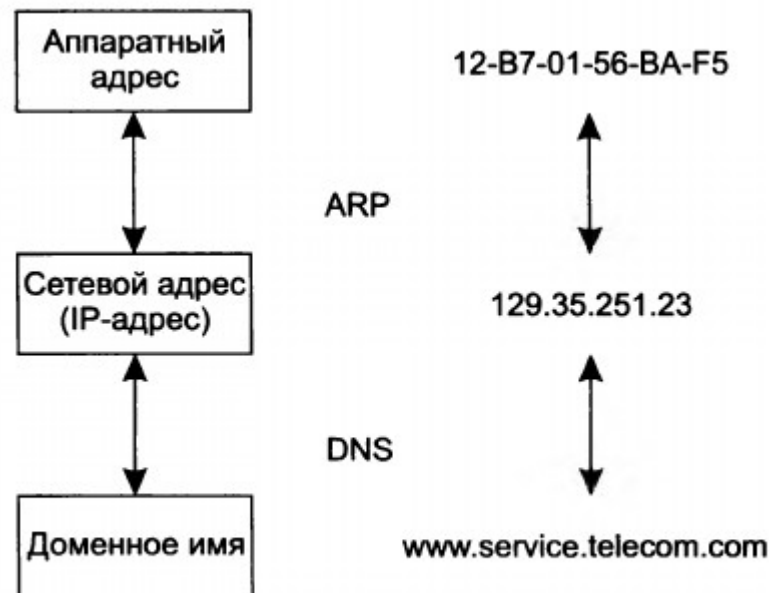


Рис. 14.3. Преобразование адресов

Формат IP-адреса

В заголовке IP -пакета предусмотрены поля для хранения IP -адреса отправителя и IP-адреса получателя. Каждое из этих полей имеет фиксированную длину 4 байта (32 бита).

Как уже было сказано, IP -адрес состоит из двух логических частей —номера сети и номера узла в сети.

Наиболее распространенной формой представления IP -адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например:

128.10.2.30

Этот же адрес может быть представлен в двоичном формате:

10000000 00001010 00000010 00011110

А также в шестнадцатеричном формате:

80.0A.02.1D

Формат IP-адреса

Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Каким образом маршрутизаторы определяют, какая часть из 32 бит, отведенных под IP -адрес, относится к номеру сети, а какая — к номеру узла?

Можно предложить несколько вариантов решения этой проблемы.

- Простейший из них состоит в использовании фиксированной границы.
- Второй подход основан на применении **маски**, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла. При таком подходе адресное пространство можно использовать для создания множества сетей разного размера.

Маска — это число, применяемое в паре с IP -адресом, причем двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые должны в IP -адресе интерпретироваться как номер сети.

- Способ, основанный на **классах адресов**. Этот способ представляет собой компромисс по отношению к двум предыдущим: размеры сетей хотя и не могут быть произвольными, как при использовании масок, но и не должны быть одинаковыми, как при установлении фиксированных границ. Вводится пять классов адресов: А, В, С, D, Е. Три из них — А, В и С — предназначены для адресации сетей, а два — D и Е — имеют специальное назначение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и номером узла.

Классы IP-адресов

1 байт		2 байт		3 байт		4 байт	
0	Номер сети (7 бит)			Номер узла (24 бит)			
Адреса класса А							
1	0	Номер сети (14 бит)		Номер узла (24 бит)			
Адреса класса В							
1	1	0	Номер сети (21 бит)			Номер узла (8 бит)	
Адреса класса С							
1	1	1	0		Групповой адрес (28 бит)		
Адреса класса D							
1	1	1	0	1	Зарезервированные адреса (27 бит)		
Адреса класса E							

Рис. 14.4. Классы IP-адресов

Классы IP-адресов

Таблица 14.1. Классы IP-адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0 (0 — не используется)	126.0.0.0 (127 — зарезервирован)	2^{24} , поле 3 байта
B	10	128.0.0.0	191.255.0.0	2^{16} , поле 2 байта
C	110	192.0.0.0	223.255.255.0	2^8 , поле 1 байт
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано

Особые IP-адреса

В TCP/IP существуют ограничения при назначении IP -адресов, а именно номера сетей и номера узлов не могут состоять из одних двоичных нулей или единиц. Введя эти ограничения, разработчики технологии TCP/IP получили возможность расширить функциональность системы адресации следующим образом:

- Если IP -адрес состоит только из двоичных нулей, то он называется неопределенным адресом и обозначает адрес того узла, который сгенерировал этот пакет. Адрес такого вида в особых случаях помещается в заголовок IP -пакета в поле адреса отправителя.
- Если в поле номера сети стоят только нули, то по умолчанию считается, что узел на значения принадлежит той же самой сети, что и узел, который отправил пакет. Такой адрес также может быть использован только в качестве адреса отправителя.
- Если все двоичные разряды IP -адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такой адрес называется ограниченным широковещательным (limited broadcast). Ограниченность в данном случае означает, что пакет не выйдет за границы данной подсети ни при каких условиях.
- Если в поле адреса назначения в разрядах, соответствующих номеру узла, стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети, номер которой указан в адресе назначения. Например, пакет с адресом 192.190.21.255 будет направлен всем узлам сети 192.190.21.0. Такой тип адреса называется широковещательным (broadcast).

Особые IP-адреса

Особый смысл имеет IP -адрес, первый октет которого равен 127. Этот адрес является внутренним адресом стека протоколов компьютера (или маршрутизатора). Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере.

Маршрут перемещения данных образует «петлю», поэтому этот адрес называется адресом обратной петли (loopback).

Использование масок при IP-адресации

Снабжая каждый IP -адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой.

Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде IP-адрес 129.64.134.5 равен:

10000001. 01000000. 10000110. 00000101,

В то время как маска 255.255.128.0 выглядит так:

11111111. 11111111. 10000000.00000000.

Если игнорировать маску и интерпретировать адрес 129.64.134.5 на основе классов, то номером сети является 129.64.0.0, а номером узла — 0.0.134.5 (поскольку адрес относится к классу B).

Если же использовать маску, то 17 последовательных двоичных единиц в маске 255.255.128.0, «наложенные» на IP-адрес 129.64.134.5, делят его на две части:

- номер сети: 10000001.01000000.1;
- номер узла: 0000110.00000101.

В десятичной форме записи номера сети и узла, дополненные нулями до 32 бит, выглядят

соответственно как 129.64.128.0 и 0.0.6.5.

Использование масок при IP-адресации

Класс адресов	Десятичная форма	Двоичная форма	Шестнадцатеричная форма	Префикс
A	255.0.0.0	11111111. 00000000. 00000000. 00000000	FF.00.00.00	/8
B	255.255.0.0	11111111. 11111111. 00000000. 00000000	FF.FF.00.00	/16
C	255.255.255.0	11111111. 11111111. 11111111. 00000000	FF.FF.FF.00	/24

Централизованное распределение адресов

В больших сетях, подобных Интернету, уникальность сетевых адресов гарантируется централизованной иерархически организованной системой их распределения. Номер сети может быть назначен только по рекомендации специального подразделения Интернета.

Главным органом регистрации глобальных адресов в Интернете с 1998 года является неправительственная некоммерческая организация **ICANN** (Internet Corporation for Assigned Names and Numbers). Эта организация координирует работу региональных отделов, деятельность которых охватывает большие географические площади: **ARIN** (Америка), **RIPE** (Европа), **APNIC** (Азия и Тихоокеанский регион).

Отображение IP-адресов на локальные адреса

Чтобы локальная технология сети смогла доставить пакет следующему маршрутизатору, необходимо:

- упаковать пакет в кадр соответствующего для данной сети формата (например, Ethernet);
- снабдить данный кадр локальным адресом следующего маршрутизатора.

Решением этих задач занимается уровень сетевых интерфейсов стека TCP/IP.

Для определения локального адреса по IP -адресу используется протокол разрешения адресов (Address Resolution Protocol, ARP).

Отображение IP-адресов на локальные адреса

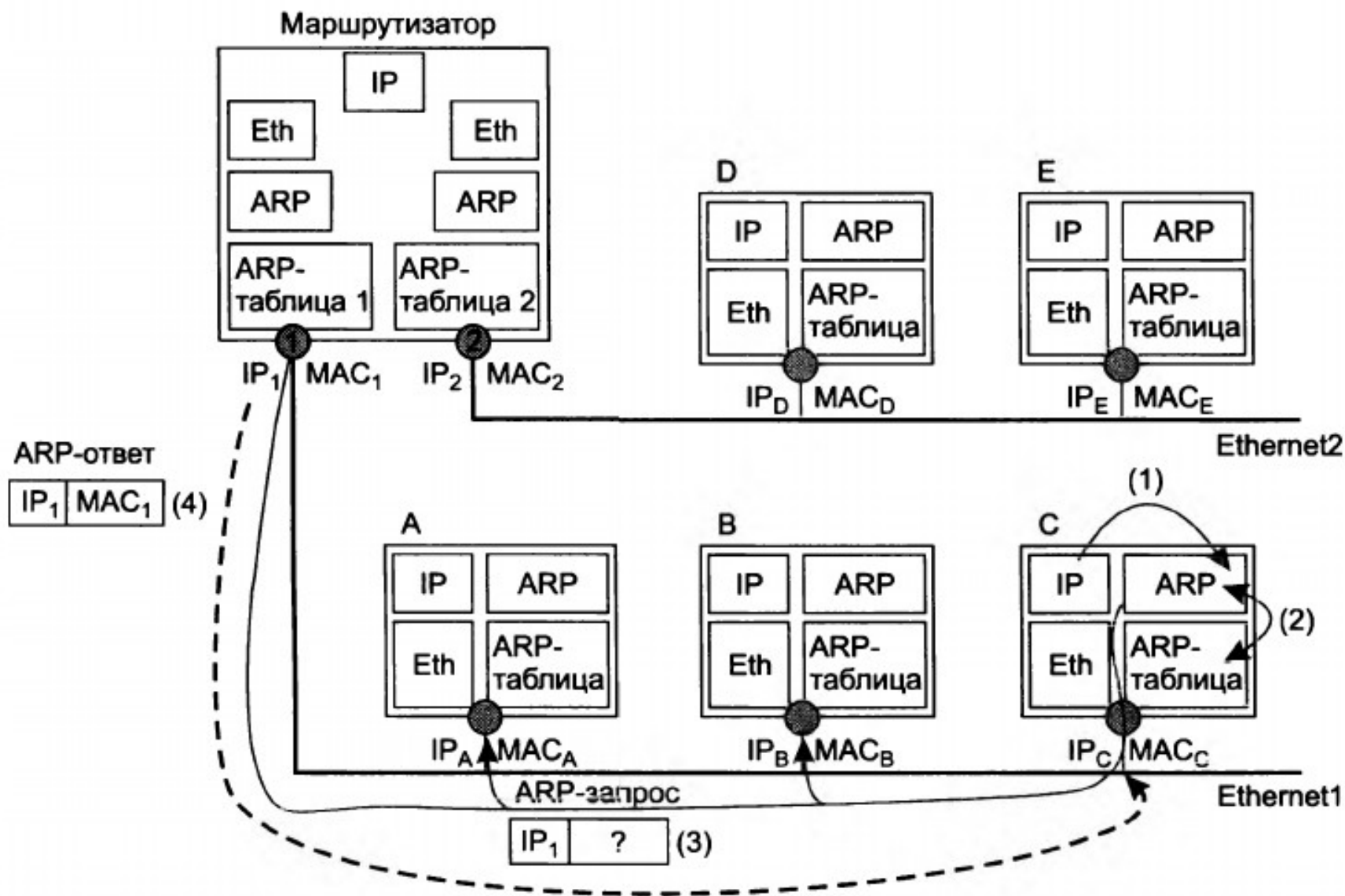


Рис. 14.7. Схема работы протокола ARP

Система DNS. Пространство DNS-имен

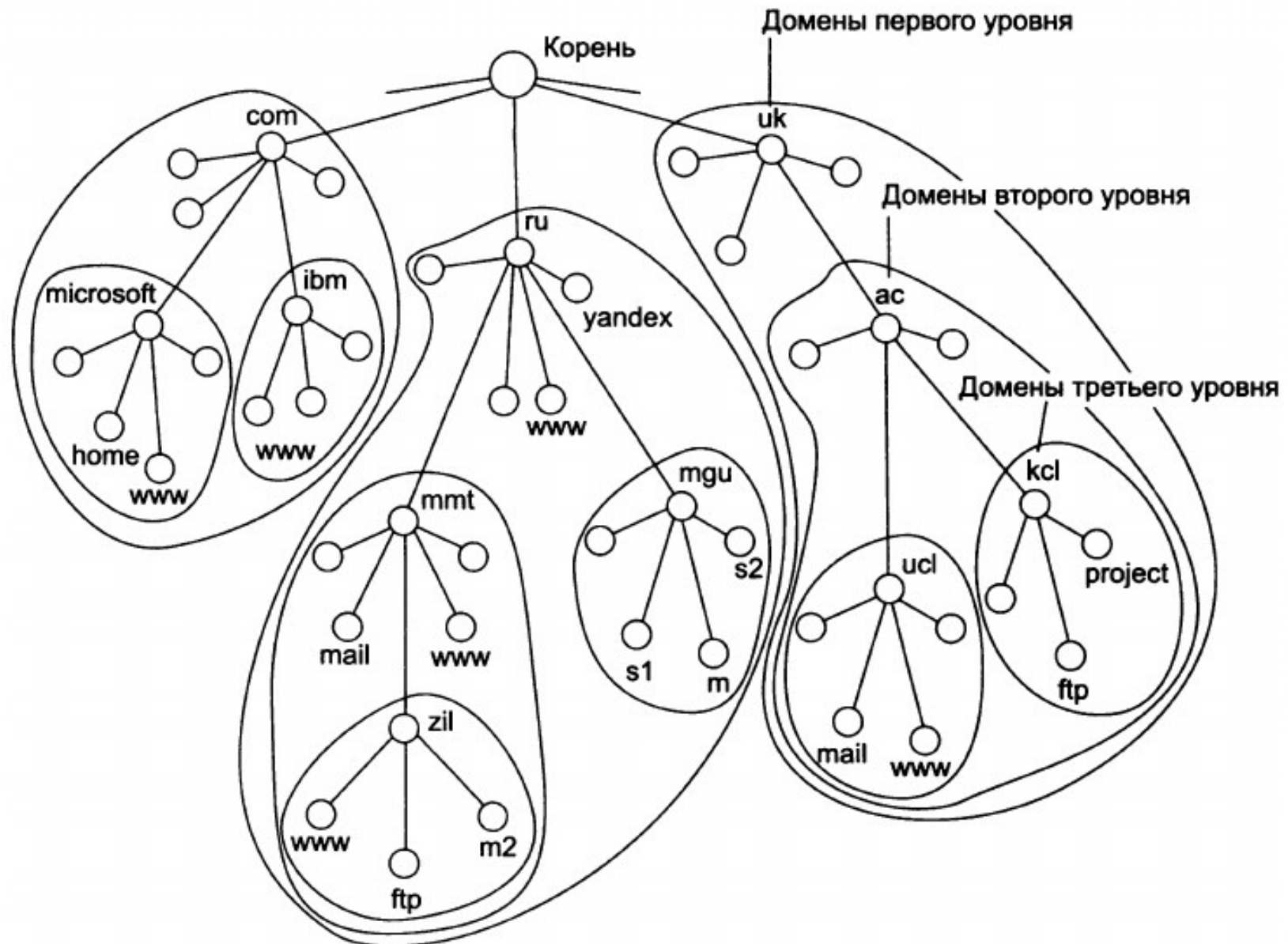


Рис. 14.10. Пространство доменных имен

Система DNS. Пространство DNS-имен

Корневой домен управляется центральными органами Интернета организацией ICANN.

Домены верхнего уровня назначаются для каждой страны, а также для различных типов организаций. Имена этих доменов должны следовать международному стандарту ISO 3166.

Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, например ru (Россия), uk (Великобритания), fi (Финляндия), us (Соединенные Штаты), а для различных типов организаций, например, следующие обозначения:

- com — коммерческие организации (например, microsoft.com);
- edu — образовательные организации (например, mit.edu);
- gov — правительственные организации (например, nsf.gov);
- org — некоммерческие организации (например, fidonet.org);
- net — сетевые организации (например, nsf.net).

Система DNS. Пространство DNS-имен

Часть пространства доменных имен, для которых некоторый DNS-сервер имеет полную информацию об их отображениях на основе соответствующего текстового файла, называется зоной DNS, а сам текстовый файл — файлом зоны. Когда DNS-сервер дает ответ о записи, входящей в зону, за которую он отвечает, такой ответ называется полномочным (authoritative) ответом DNS. Как мы увидим далее, DNS-сервер может также давать неполномочный ответ, если запрос относится не к его зоне, но он знает его за счет кэширования ответов других серверов. Заметим, что DNS-сервер может обслуживать несколько зон.

Файл зоны состоит из текстовых записей нескольких типов, таких как:

- A — отображает имя на IPv4 адрес;
- AAAA — отображает имя на IPv6 адрес;
- NS — определяет имя DNS-сервера для некоторого домена;
- MX — определяет имя почтового сервера для некоторого домена.

Существуют записи и некоторых других типов.

Система DNS. Пространство DNS-имен

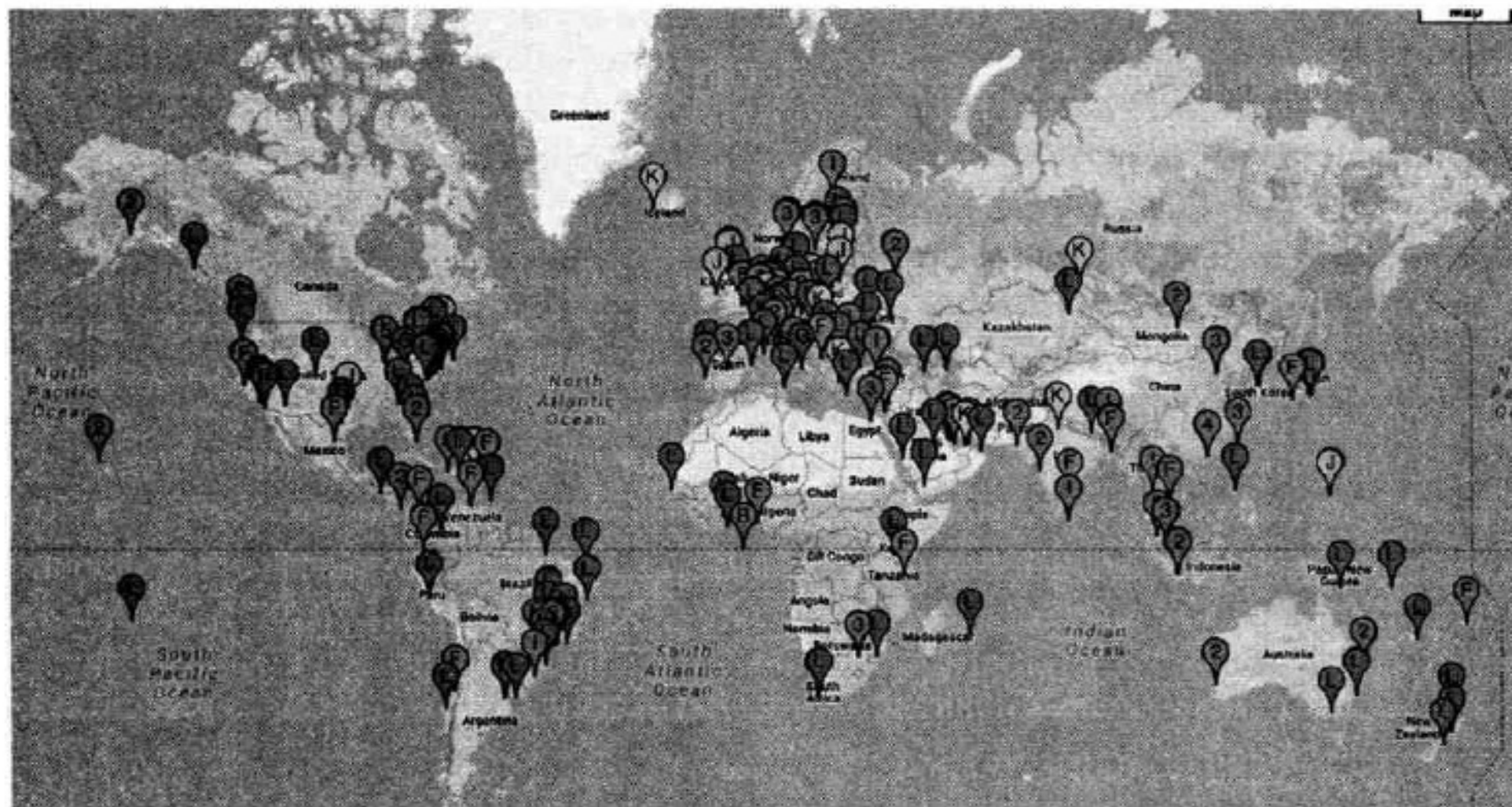


Рис. 14.11. Географическое распределение корневых серверов DNS (источник: root-servers.org)

Протокол DHCP

Протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCP) автоматизирует процесс конфигурирования сетевых интерфейсов, гарантируя от дублирования адресов за счет централизованного управления их распределением.

При этом DHCP-сервер может работать в разных режимах, включая:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

Алгоритм динамического назначения адресов

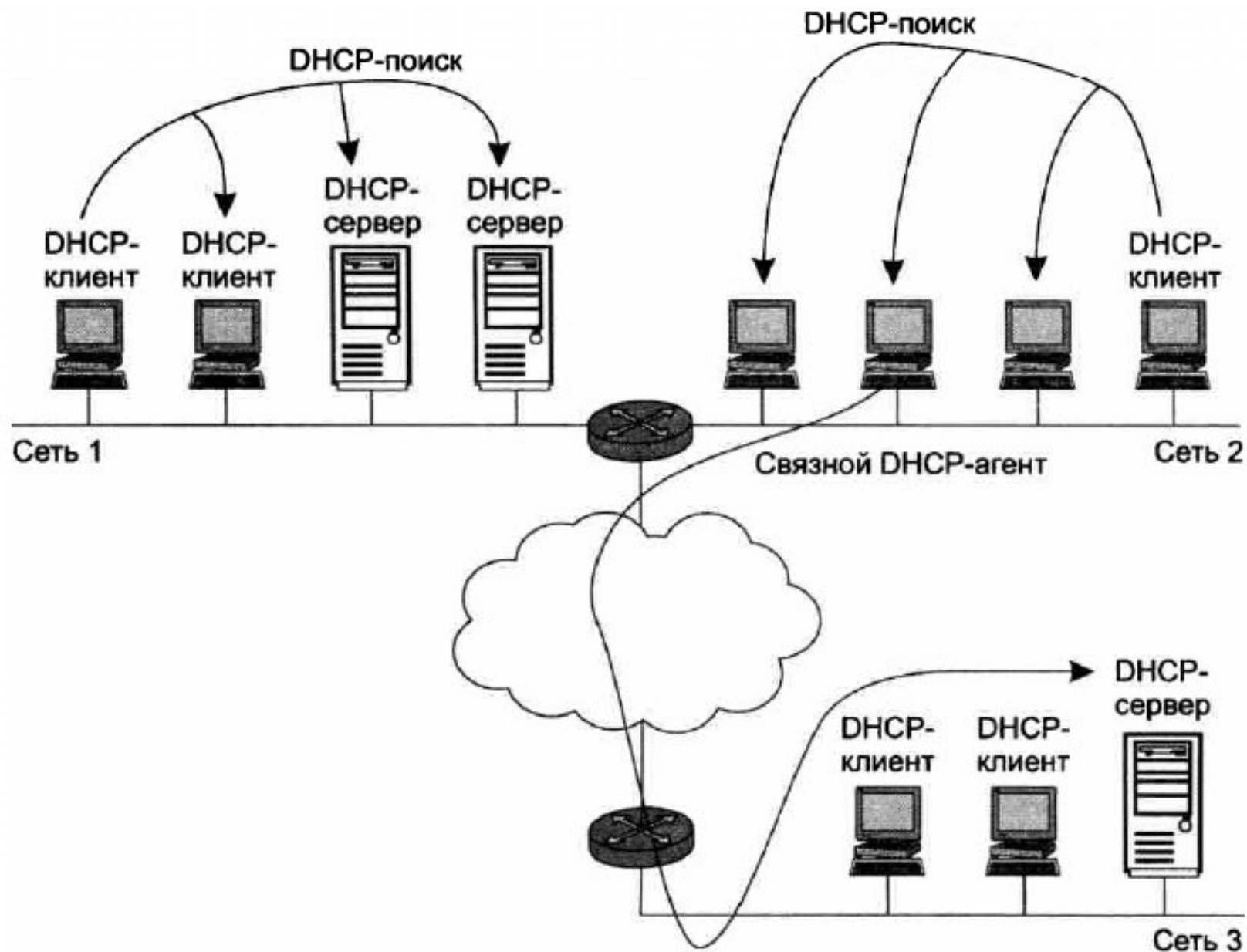


Рис. 14.12. Схемы взаимного расположения DHCP-серверов и DHCP-клиентов