

IP-сети

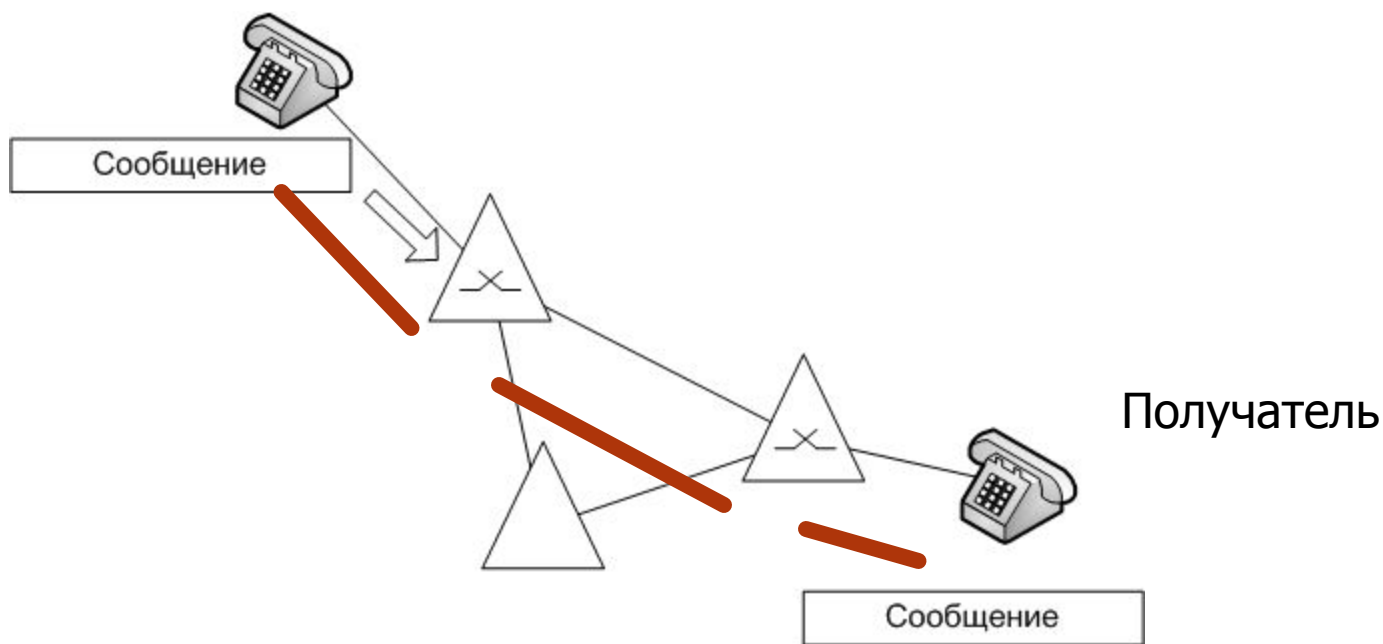
IP-сети, как основа сетей IP-телефонии .

Часть 1

Сети коммутации пакетов

Коммутация каналов

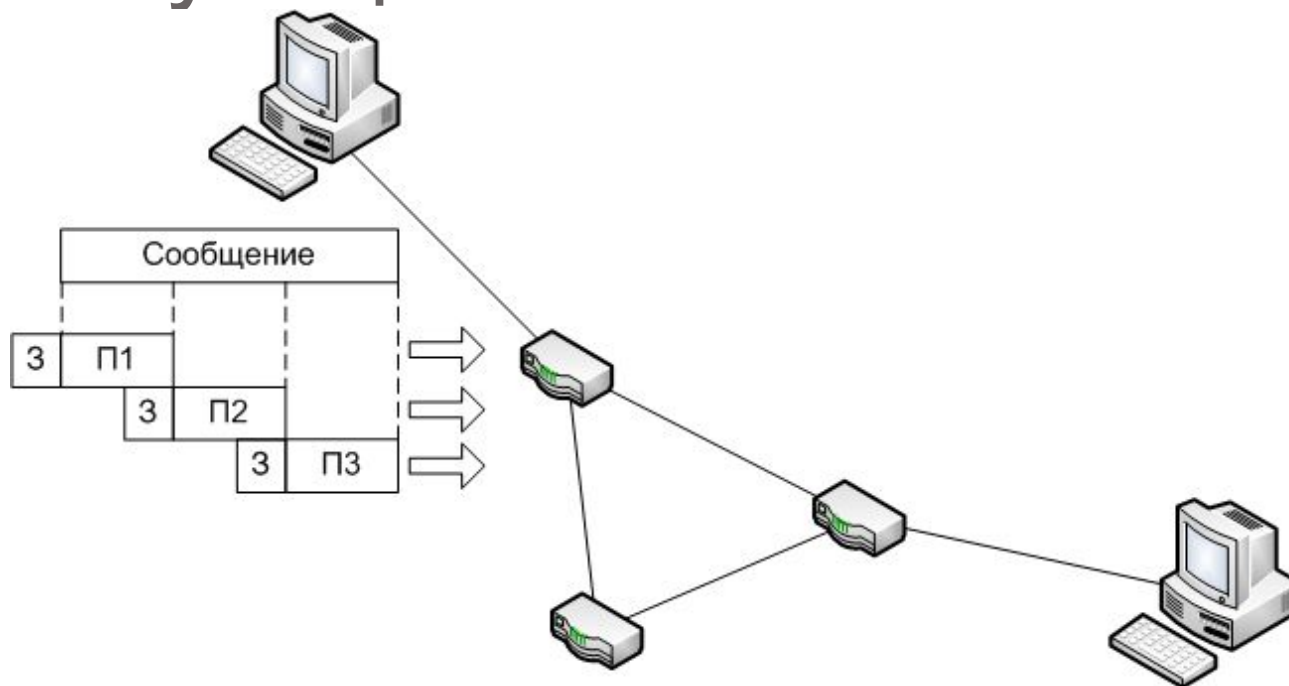
Отправитель



Действия для передачи сообщения:

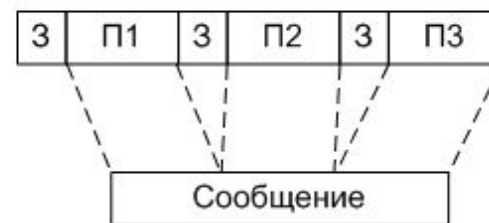
- 1) Установить канал
- 2) Передать сообщение
- 3) Разрушить канал

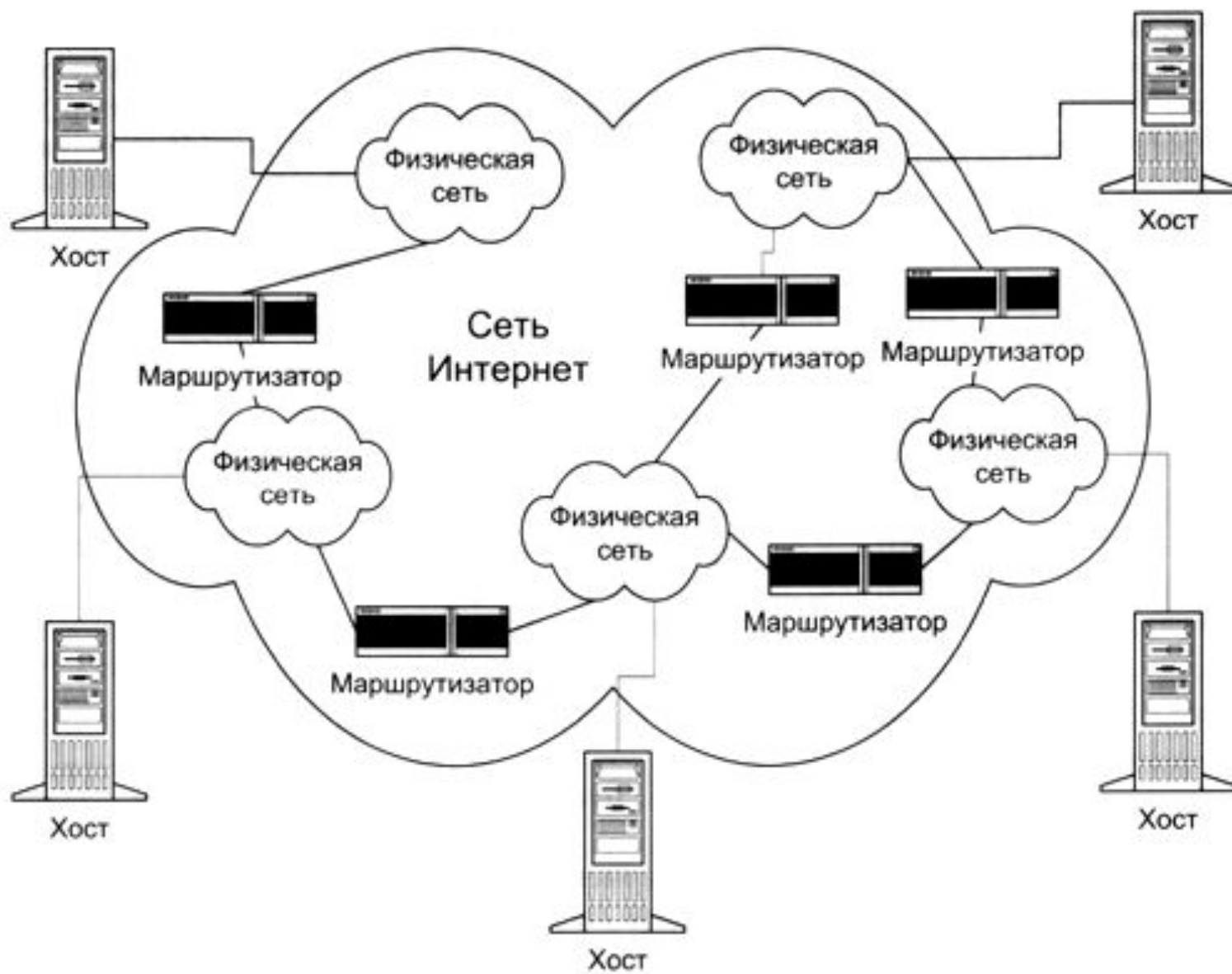
Коммутация пакетов



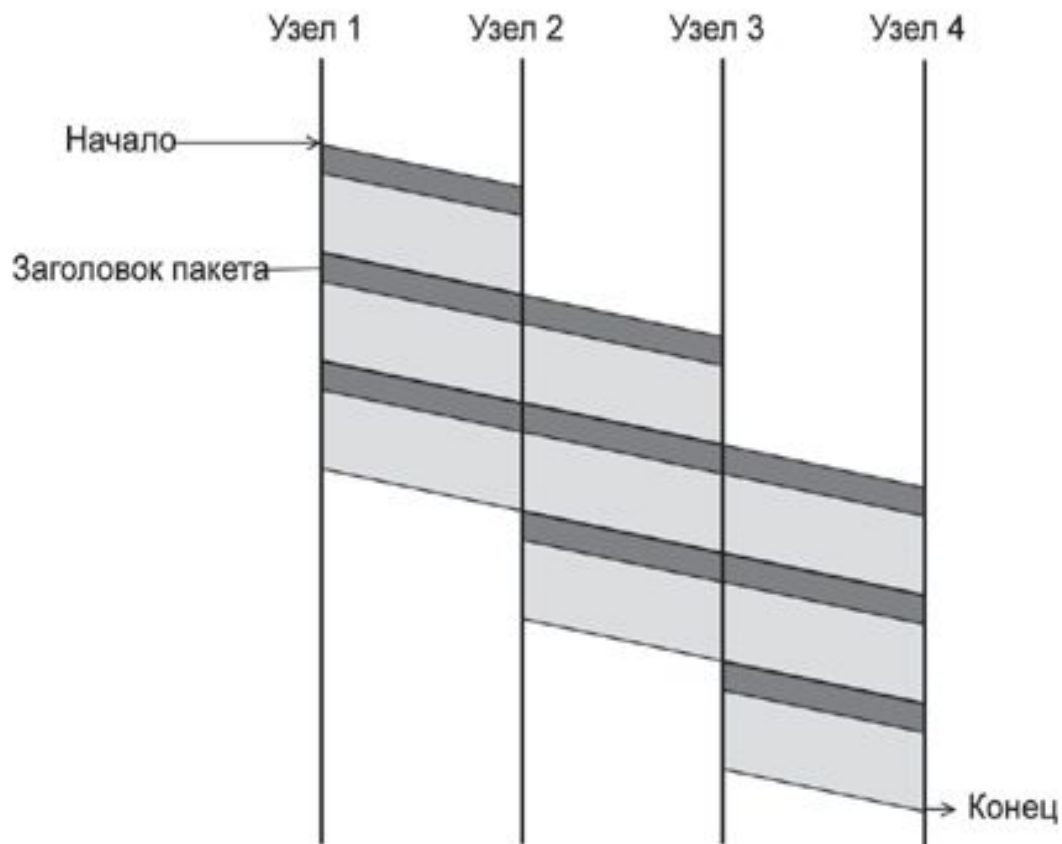
Действия для передачи сообщения:

- 1) Сформировать пакеты: порезать сообщение на порции, снабдить каждую заголовком
- 2) Передать пакеты через сеть
- 3) Собрать из пакетов исходное сообщение



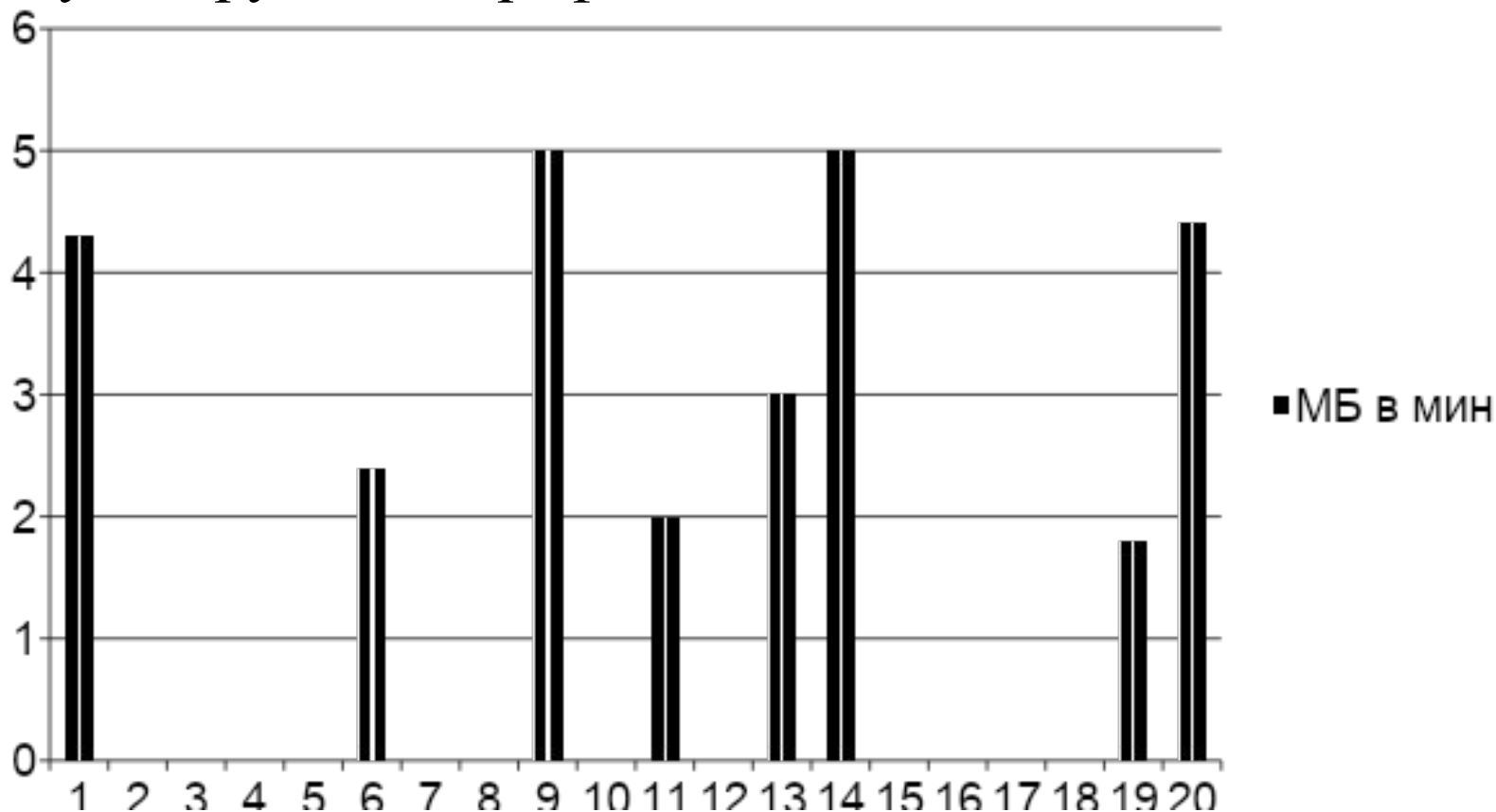


Передача пакетов по сети с задержкой

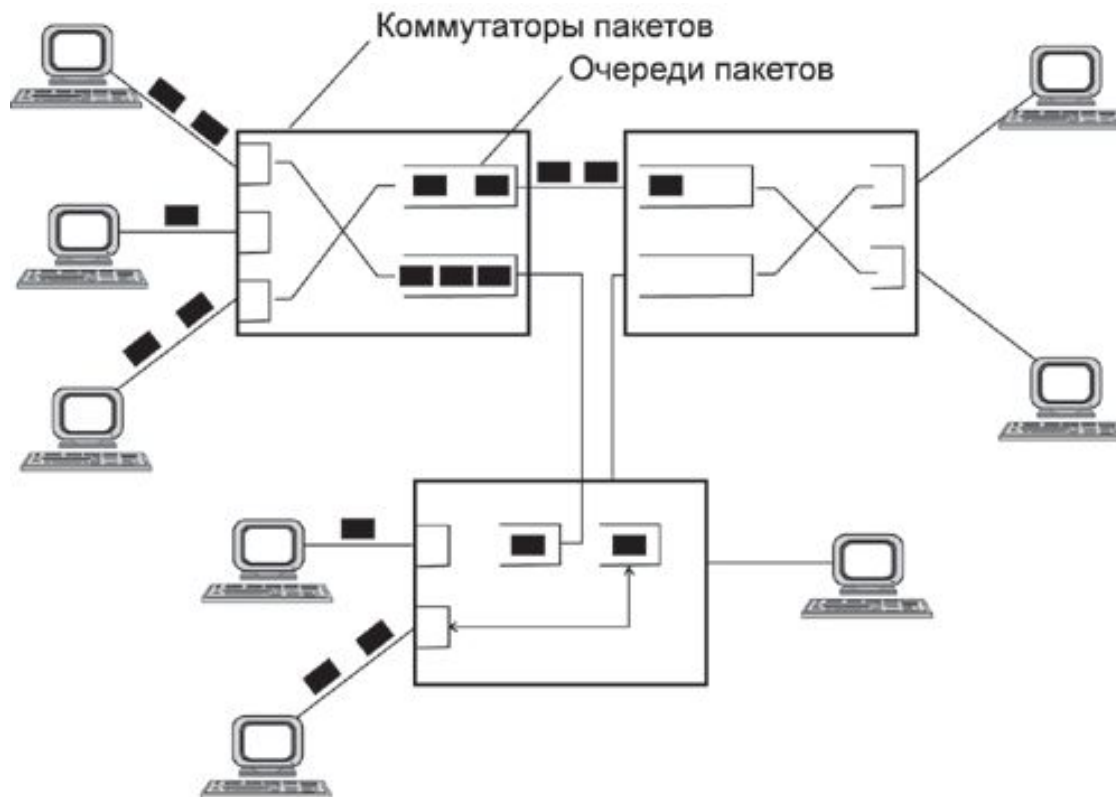


Передача данных в компьютерных сетях

- Пульсирующий трафик



Сеть с коммутацией пакетов должна сглаживать пульсации



- Данные нарезаются порциями - пакетами, каждый из которых обрабатывается коммутаторами независимо
- Каждый пакет содержит адрес назначения и адрес отправителя
- Не требуется предварительной процедуры установления соединения

Сравнение технологий

Коммутация каналов

- С установлением соединения
- Задержка определяется скоростью распространения
- Канал устанавливается на все время соединения

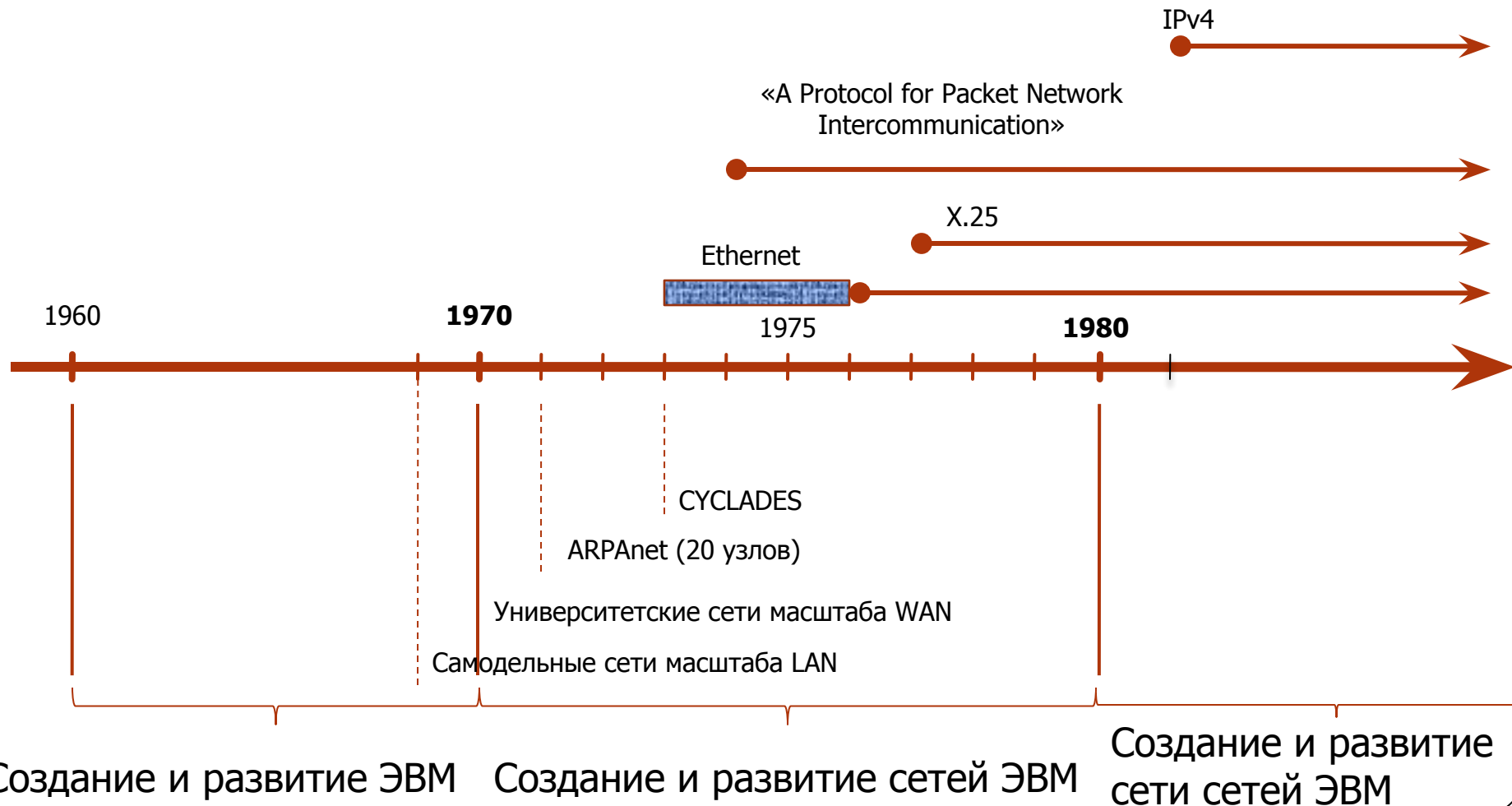
Коммутация пакетов

- Без установления соединения
- Задержка определяется количеством узлов и уровнем их загрузки
- Передача пакетов производится только при наличии информации для передачи

Часть 2

Введение в IP-сети

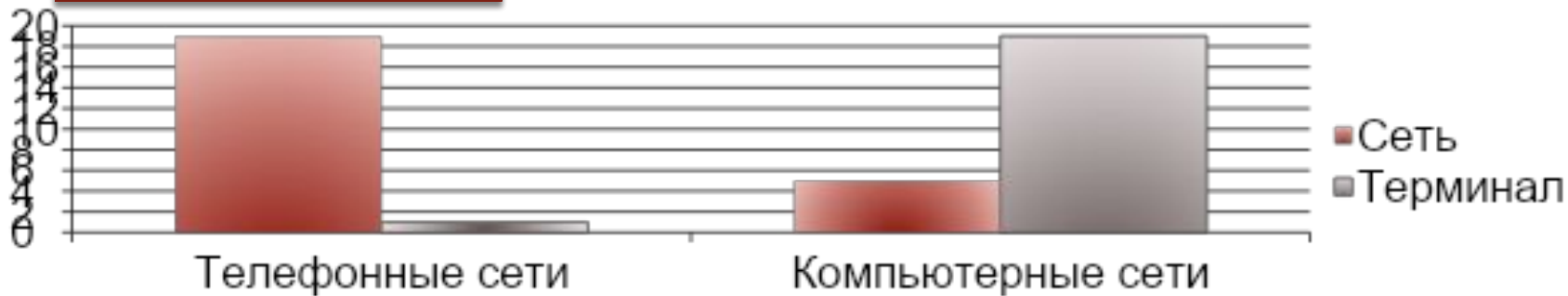
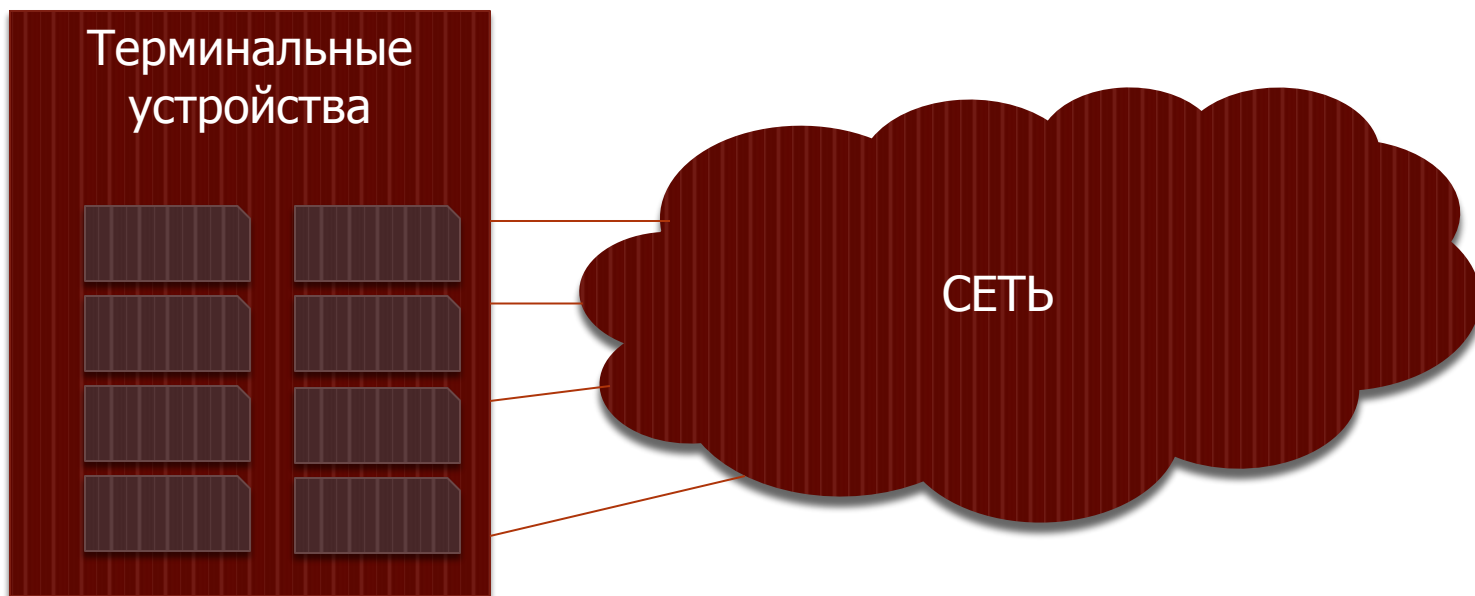
История возникновения сетей передачи данных

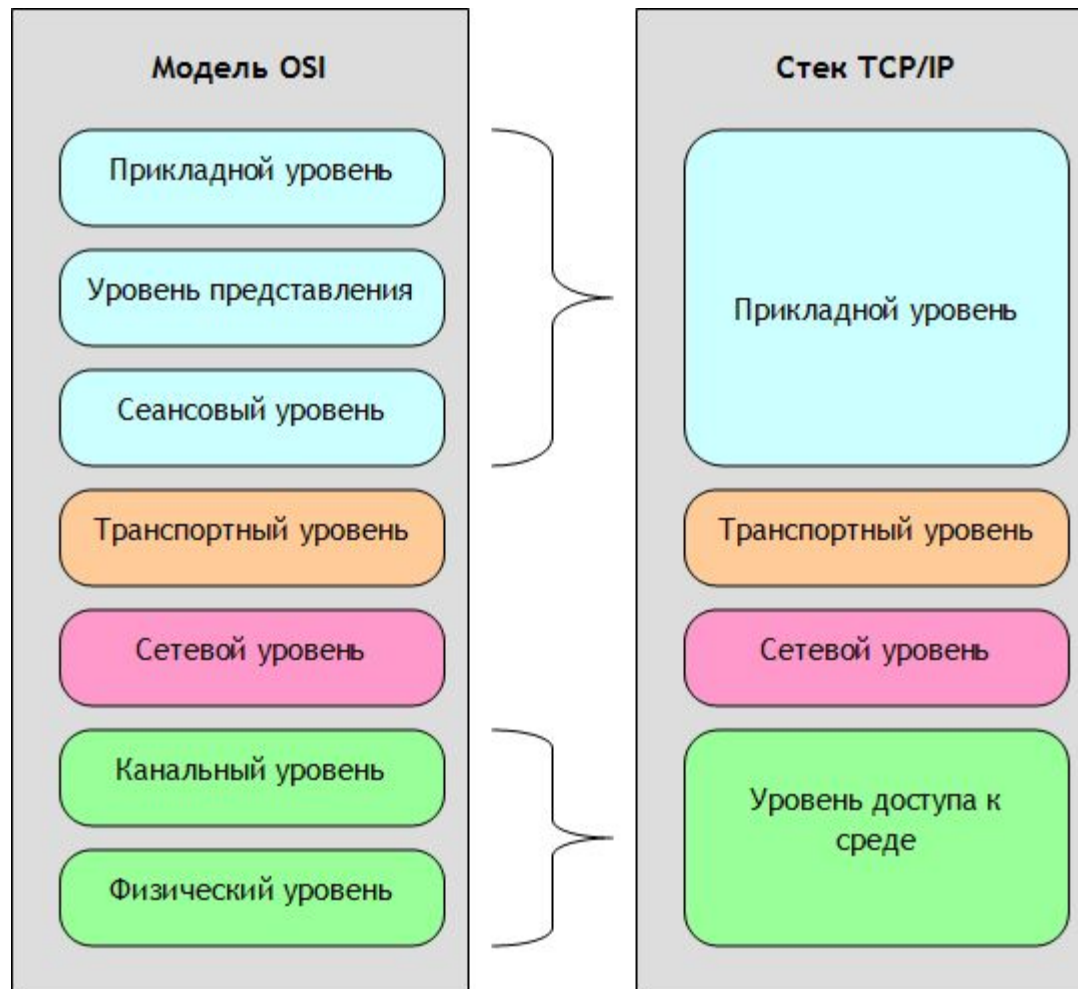


История возникновения IP-сетей

- 70-е гг. Агентство Передовых Проектов Национальной Безопасности США (US Defense Advanced Research Project Agency – DARPA) занимается разработкой сети
- 1971 – в ARPAnet ~ 20 узлов
- Передача ведётся при помощи NCP (Network Communication Protocol)
- 1974 – появление протокола TCP
- 1978 – разделение на TCP и IP.
- 1983 – ARPAnet => DARPAnet и MILnet
- 1984 – Появление системы доменных имён DNS
- 1990 – Исчезновение ARPAnet
- 1991 – Всемирная паутина WWW

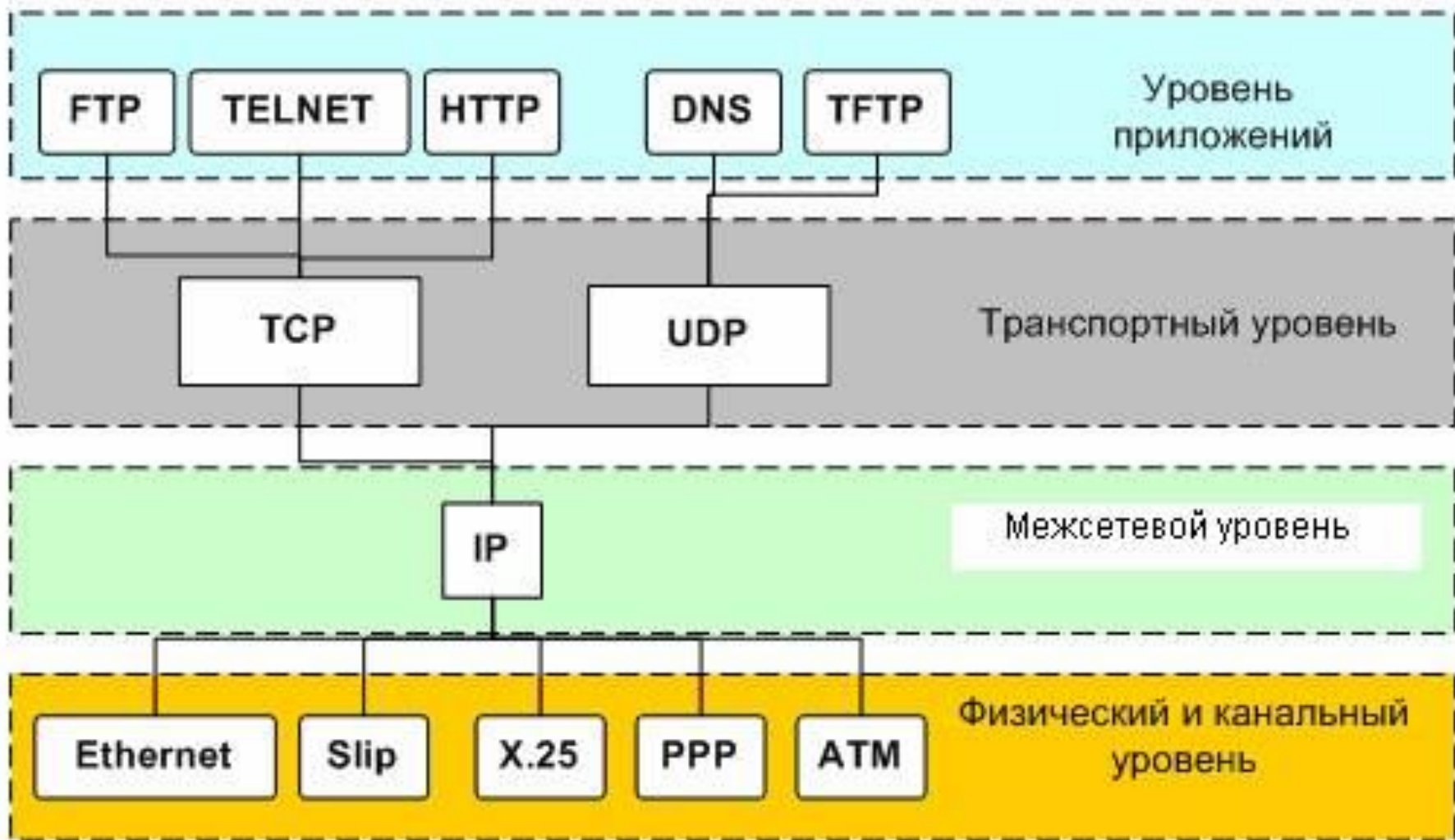
Перераспределение сетевых функций



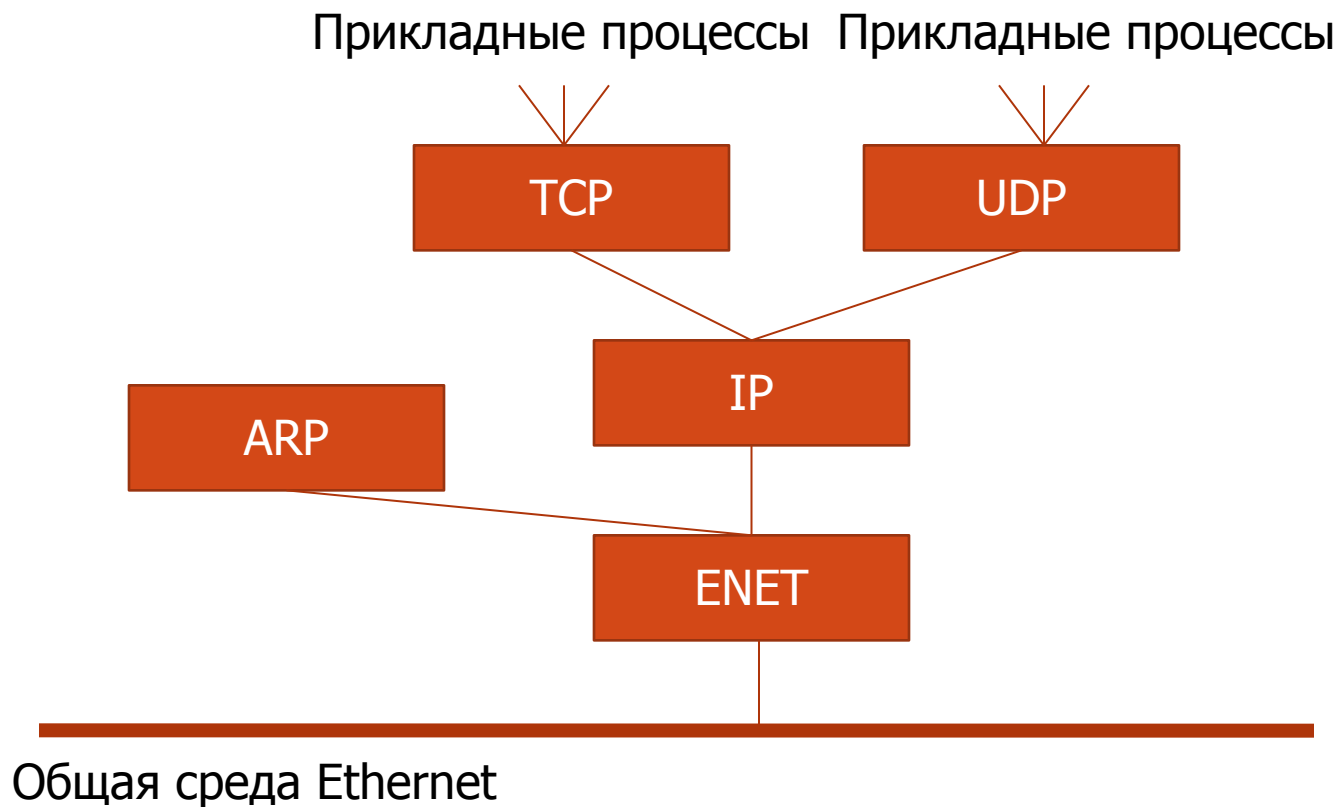


Распределение протоколов по уровням модели TCP/IP

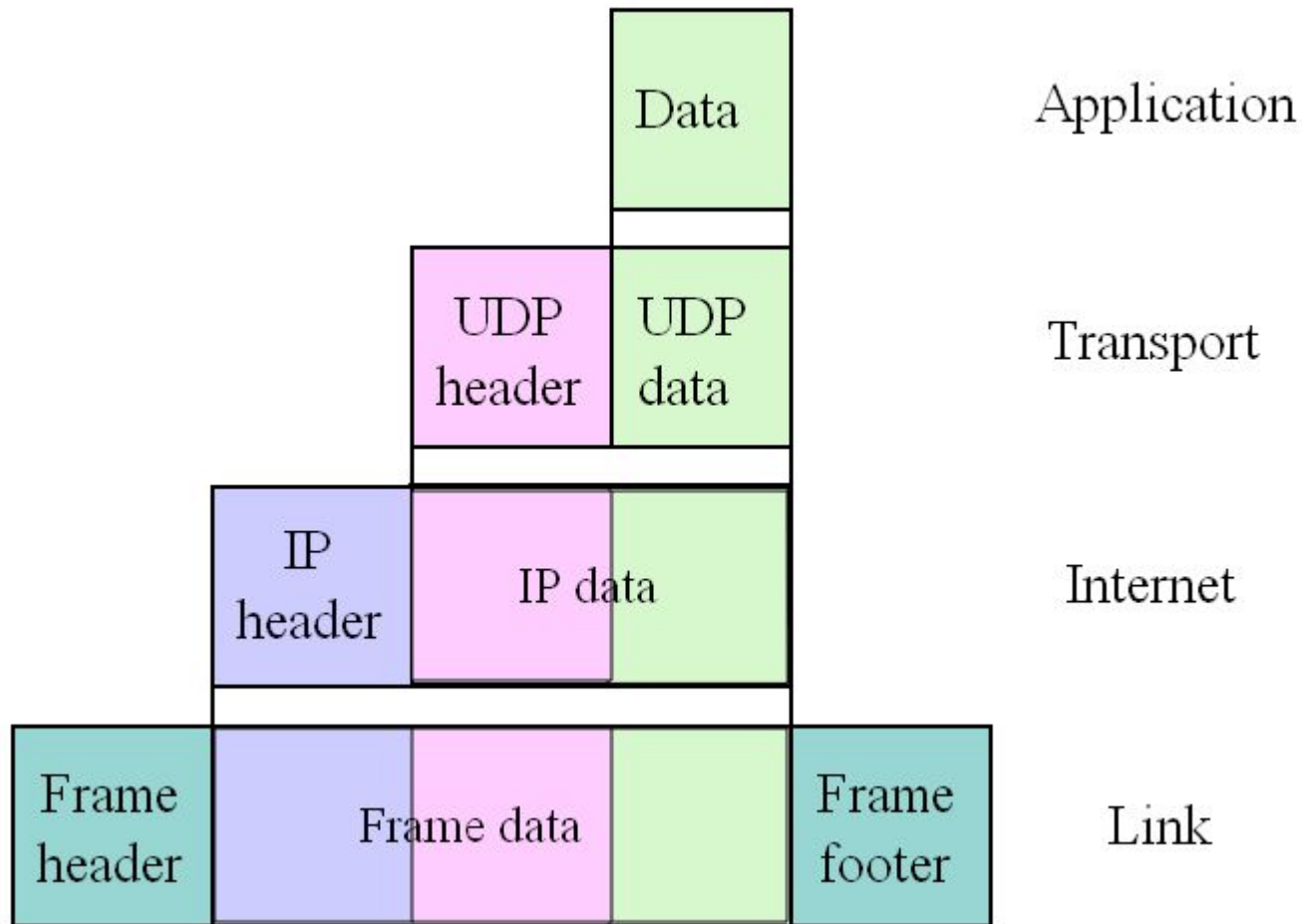
5	Прикладной <i>«7 уровень»</i>	напр., HTTP, RTP, FTP, DNS <i>(RIP, работающий поверх UDP, и BGP, работающий поверх TCP, являются частью сетевого уровня)</i>
4	Транспортный	напр., TCP, UDP, SCTP, DCCP <i>(протоколы маршрутизации, подобные OSPF, что работают поверх IP, являются частью сетевого уровня)</i>
3	Сетевой	Для TCP/IP это IP (IP) <i>(вспомогательные протоколы, вроде ICMP и IGMP, работают поверх IP, но тоже относятся к сетевому уровню; протокол ARP является самостоятельным вспомогательным протоколом, работающим поверх физического уровня)</i>
2	Канальный	Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM и MPLS
1	Физический	напр., физическая среда и принципы кодирования информации, T1, E1



Структура связей протокольных модулей



Инкапсуляция информации

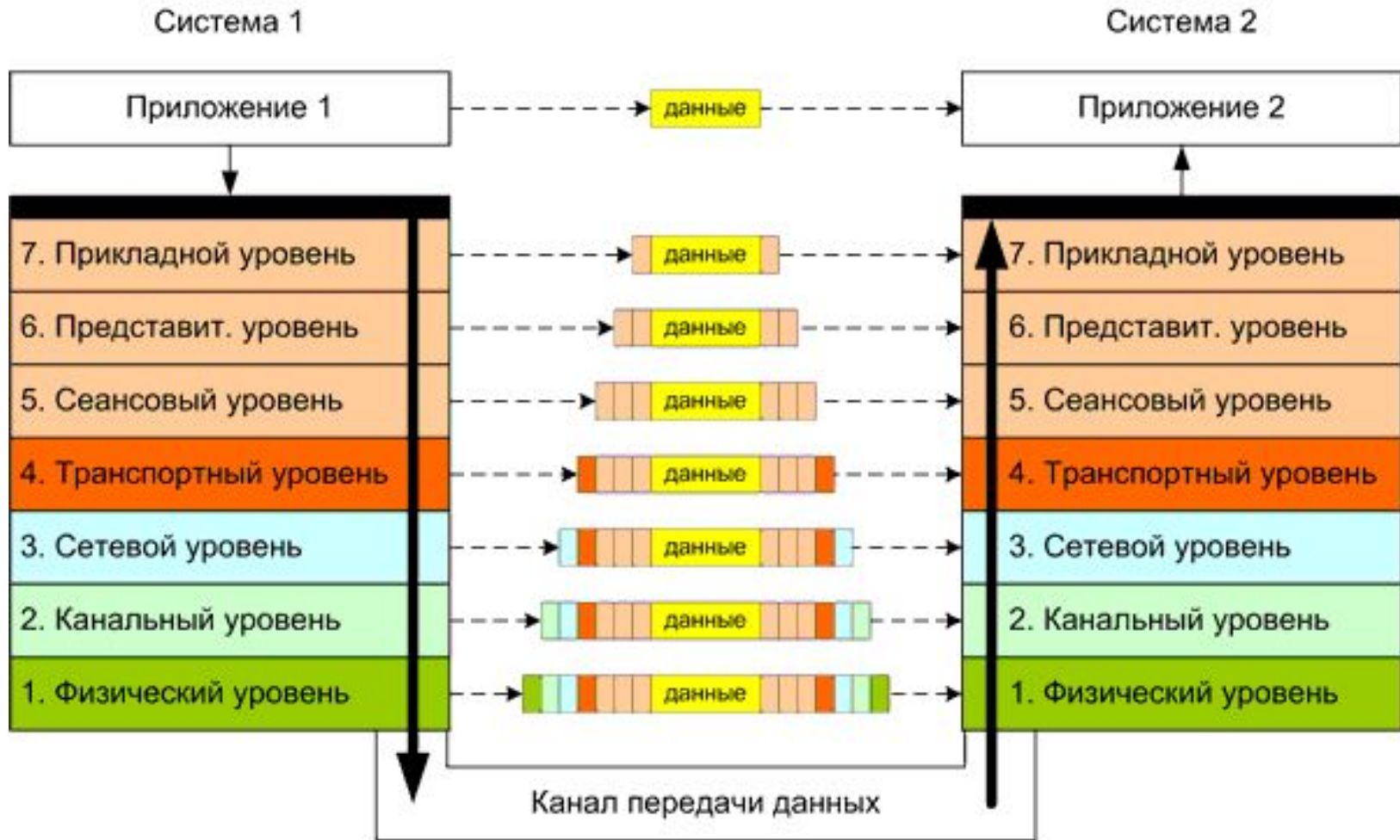


Принцип построения IP сети

Модель OSI

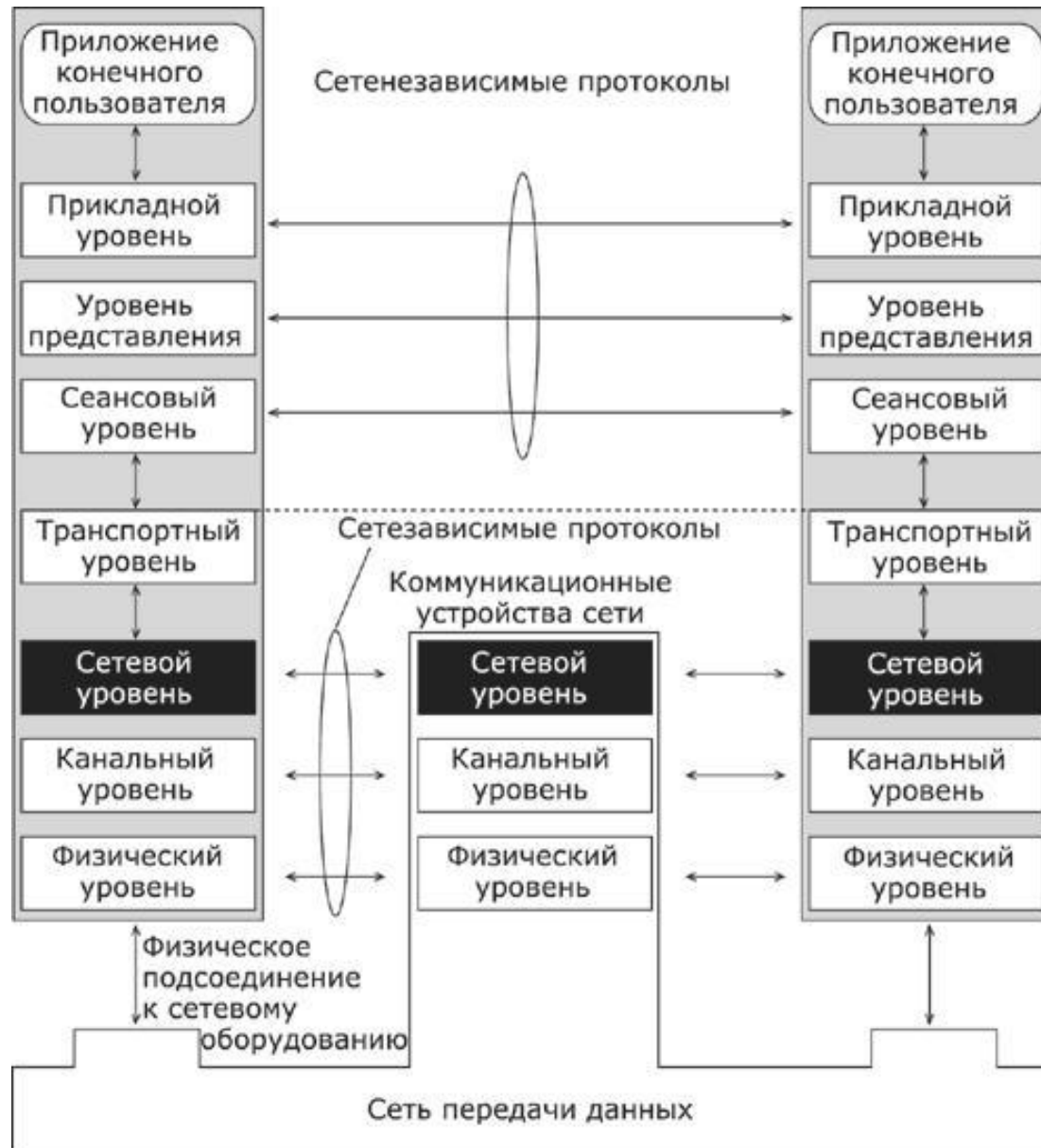


Модель OSI



- Логическое соединение между уровнями
- Реализация передачи данных

Модель OSI



Работа приложений



Сеть IP

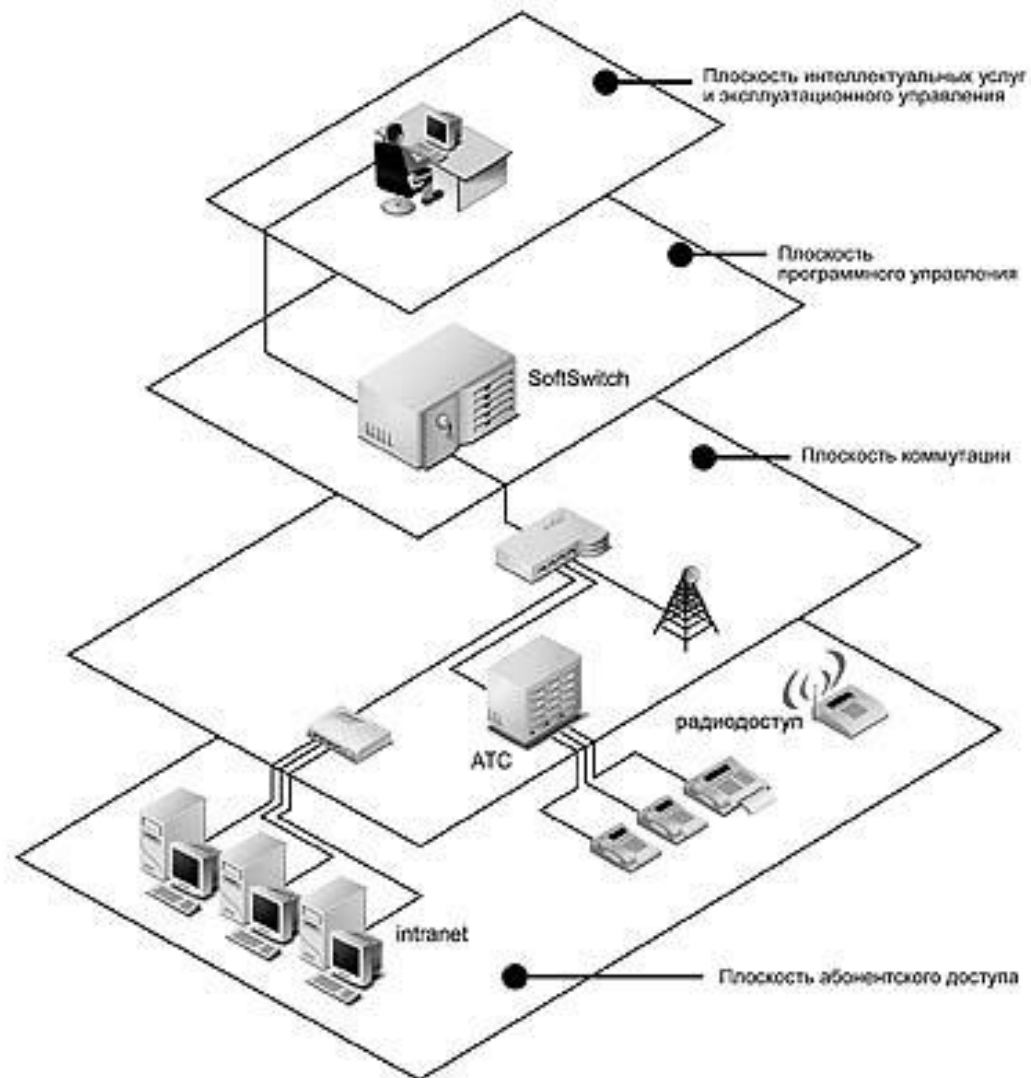
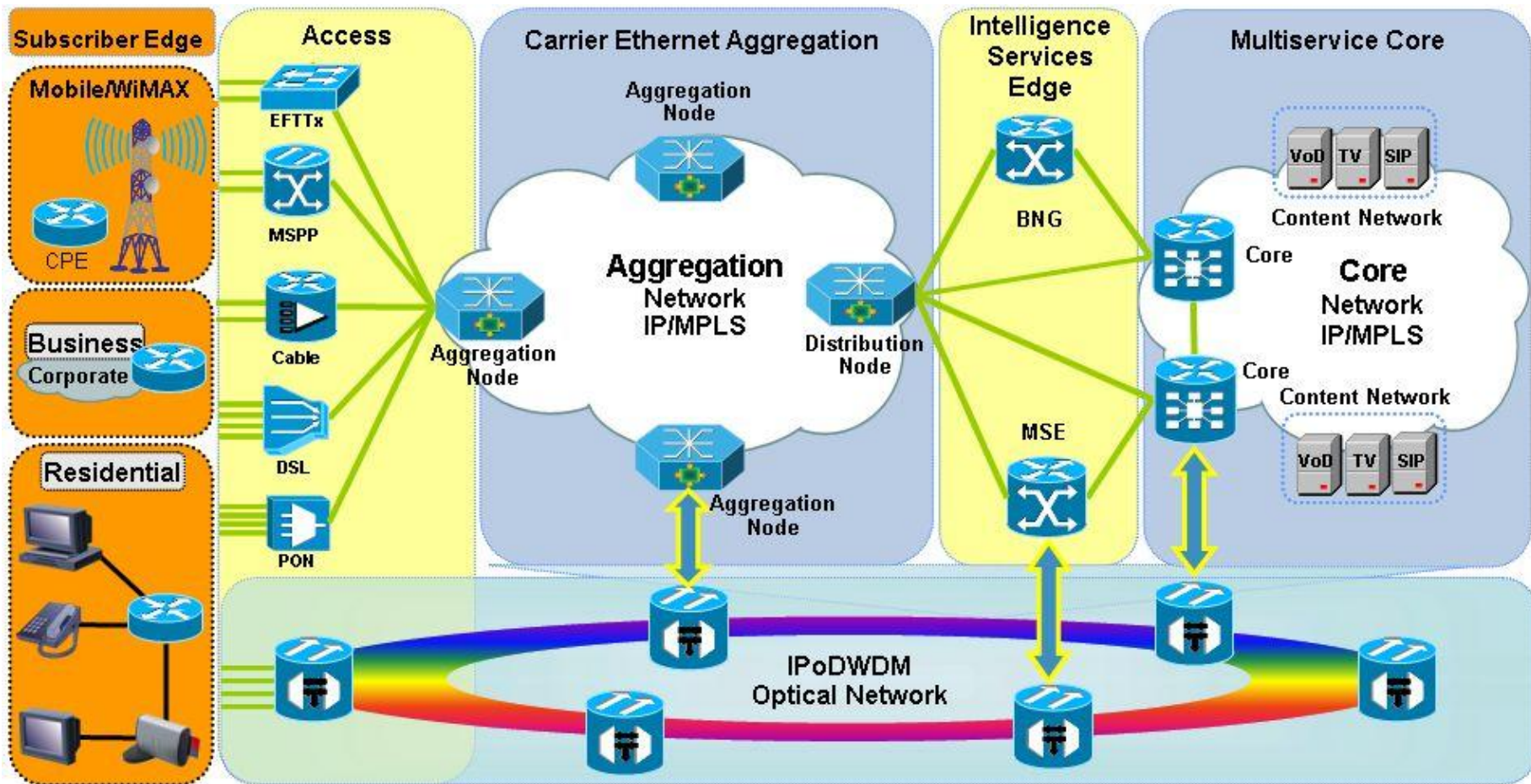


Рис. 1

Сеть IP



Основные виды оборудования современных сетей передачи данных

Коммутатор

- устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.
- передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых не известен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор

- Коммутатор хранит в памяти таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора.
- При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры (фреймы) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время.
- Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице.
- Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен.
- Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется. Стоит отметить малую латентность (задержку) и высокую скорость пересылки на каждом порту интерфейса..

Коммутатор

- существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.
- С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.
- Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.
- Бесфрагментный (fragment-free) или *гибридный*. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (кадры размером 64 байта обрабатываются по технологии store-and-forward, остальные — по технологии cut-through).
- Задержка, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него, и вместе с ним определяет общую задержку коммутатора.

Сетевой концентратор

- устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа *витая пара*. В настоящее время вытеснены сетевыми коммутаторами.
- Сетевые концентраторы также могли иметь разъёмы для подключения к существующим сетям на базе толстого или тонкого коаксиального кабеля.

Маршрутизатор

- специализированное сетевое устройство, имеющее минимум два сетевых интерфейса и пересылающее пакеты данных между различными сегментами сети, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.
- Маршрутизаторы делятся на программные и аппаратные.
- Маршрутизатор работает на более высоком «сетевом» уровне 3 сетевой модели OSI, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают на 2 уровне и 1 уровне модели OSI соответственно.

Шлюз

- аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).
- Сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды (сети).

Шлюз

- Сетевые шлюзы работают на всех известных операционных системах.
- Роутер сам по себе принимает, проводит и отправляет пакеты только среди сетей, использующих одинаковые протоколы. Сетевой шлюз может с одной стороны принять пакет, сформатированный под один протокол (например Apple Talk) и конвертировать в пакет другого протокола (например TCP/IP) перед отправкой в другой сегмент сети.
- Сетевые шлюзы могут быть аппаратным решением, программным обеспечением или тем и другим вместе, но обычно это программное обеспечение, установленное на роутер или компьютер.
- Сетевой шлюз должен понимать все протоколы, используемые роутером.
- Обычно сетевые шлюзы работают медленнее, чем сетевые мосты, коммутаторы и обычные роутеры. С
- Шлюз — это точка сети, которая служит выходом в другую сеть.

Межсетевой экран (firewall)

- комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
- Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.
- Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.

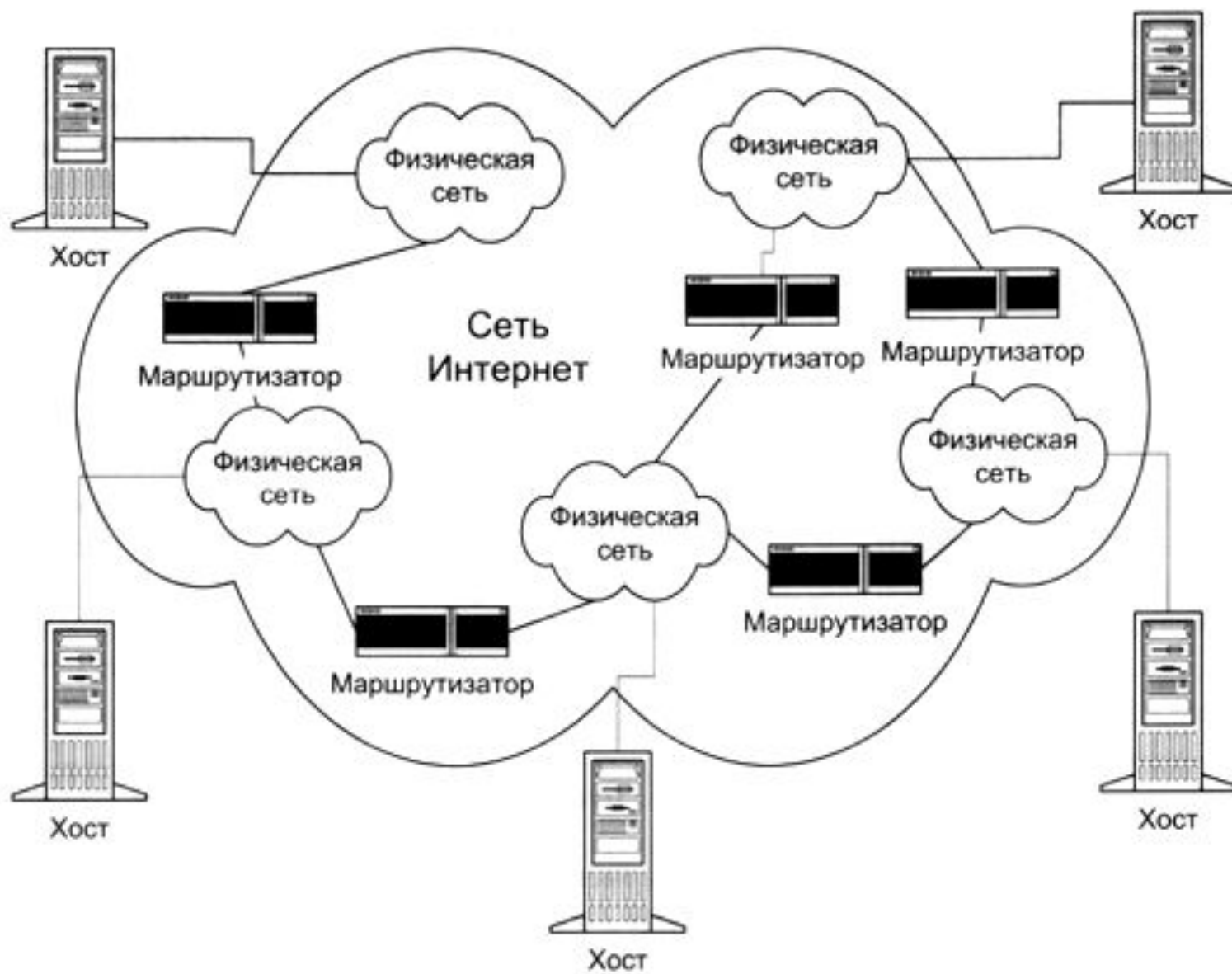
Межсетевой экран (firewall)

- Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:
 - обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;
 - на уровне каких сетевых протоколов происходит контроль потока данных;
 - отслеживаются ли состояния активных соединений или нет.
- В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:
 - *традиционный сетевой (или межсетевой) экран* — программа (или неотъемлемая часть операционной системы) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующее входящие и исходящие потоки данных между подключенными сетями.
 - *персональный сетевой экран* — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.
- В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:
 - *сетевом уровне,*
 - *сеансовом уровне*
 - *уровне приложений*
- В зависимости от отслеживания активных соединений сетевые экраны бывают:
 - *stateless* (простая фильтрация), которые не отслеживают текущие соединения (например, **TCP**), а фильтруют поток данных исключительно на основе статических правил;
 - *stateful, stateful packet inspection (SPI)* (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений.

Основные возможности Firewall

- фильтрация доступа к заведомо незащищенным службам;
- препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
- контроль доступа к узлам сети;
- может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
- регламентирование порядка доступа к сети;
- уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Классификация сетей



Сетевые архитектуры

- Звезда
- Кольцо
- Дерево
- Точка-точка
- Другие

Признаки классификации

- Все многообразие компьютерных сетей можно классифицировать по группе признаков:
 - 1) Территориальная распространенность;
 - 2) Ведомственная принадлежность;
 - 3) Скорость передачи информации;
 - 4) Тип среды передачи;
 - 5) Топология;
 - 6) Организация взаимодействия компьютеров.

По территориальной распространенности

- *По территориальной распространенности* сети могут быть локальными, глобальными, и региональными.
- **Локальные** - это сети, расположенные в пределах одного здания.

Региональные - расположенные на территории города или области.

Глобальные на территории государства или группы государств, например, всемирная сеть Internet.

Локальная сеть

- Компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Локальная сеть

- Компьютеры могут соединяться между собой, используя различные среды доступа: медные проводники (витая пара), оптические проводники (оптические кабели) и через радиоканал (беспроводные технологии). Проводные, оптические связи устанавливаются через Ethernet, беспроводные — через Wi-Fi, Bluetooth, GPRS и прочие средства. Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней.

Глобальная сеть сетей

- компьютерная сеть, охватывающая большие территории и включающая в себя большое число компьютеров.
- ГКС служат для объединения разрозненных сетей так, чтобы пользователи и компьютеры, где бы они ни находились, могли взаимодействовать со всеми остальными участниками глобальной сети.
- Некоторые ГКС построены исключительно для частных организаций, другие являются средством коммуникации корпоративных ЛВС с сетью Интернет или посредством Интернет с удалёнными сетями, входящими в состав корпоративных.
- Чаще всего ГКС опирается на выделенные линии, на одном конце которых маршрутизатор подключается к ЛВС, а на другом коммутатор связывается с остальными частями ГКС. Основными используемыми протоколами являются TCP/IP, SONET/SDH, MPLS, ATM и Frame relay. Ранее был широко распространён протокол X.25, который может по праву считаться прародителем Frame relay.

Различия глобальных и локальных сетей

- Глобальные сети отличаются от локальных тем, что рассчитаны на неограниченное число абонентов и используют, как правило, не слишком качественные каналы связи и сравнительно низкую скорость передачи, а механизм управления обменом у них в принципе не может быть гарантированно быстрым.
- В глобальных сетях намного более важно не качество связи, а сам факт ее существования. Правда, в настоящий момент уже нельзя провести четкий и однозначный предел между локальными и глобальными сетями. Большинство локальных сетей имеют выход в глобальную сеть, но характер переданной информации, принципы организации обмена, режимы доступа к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что приняты в глобальной сети. И хотя все компьютеры локальной сети в данном случае включены также и в глобальную сеть, специфику локальной сети это не отменяет. Возможность выхода в глобальную сеть остается всего лишь одним из ресурсов, поделенным пользователями локальной сети.

Классификация сетей (продолжение)

- **Ведомственная принадлежность**

- По принадлежности различают *ведомственные* и *государственные сети*. Ведомственные принадлежат одной организации и располагаются на ее территории. Государственные сети - сети, используемые в государственных структурах.

- **По скорости передачи**

- По скорости передачи информации компьютерные сети делятся на низко-, средне- и высокоскоростные.
- низкоскоростные (до 10 Мбит/с),
- среднескоростные (до 100 Мбит/с),
- высокоскоростные (свыше 100 Мбит/с);

- **По типу среды передачи**

- По типу среды передачи сети разделяются на:
- проводные – коаксиальные, на витой паре, оптоволоконные;
- беспроводные - с передачей информации по радиоканалам, в инфракрасном диапазоне.

Стек TCP/IP

Межсетевой протокол IP

- Межсетевой протокол (Internet protocol, IP) предназначен для связи сетей передачи данных, использующих коммутацию пакетов.
- Данный протокол предоставляет услуги без установления связи между источником и получателем. (протокол не отвечает за установление соединений в сети)

Межсетевой протокол IP

- Определяет форму передачи информации по IP сети;
- Устанавливает принципы адресации в глобальной сети;
- Определяет принципы маршрутизации IP пакетов.

IP среда – переносит IP пакеты к узлу, IP адрес которого указан в графе получателя.

Межсетевой протокол IP

- Среда IP – ненадежная транспортная среда.
- Нет гарантий того, что IP пакет достигнет получателя;
- Заранее неизвестно с какой задержкой пакет будет доставлен
- Порядок передачи пакетов может измениться

Межсетевой протокол IP

Все задачи, относительно:

- надежности;
- шифрования;
- мультиплексирования потоков от/идентифицирования приложений

реализуются выше стоящими протоколами

Формат пакета IP v.4

VERS (4 бита)	HLEN (4 бита)	Тип службы (8 бит)	Общая длина (16 бит)
Поле идентификации (16 бит)		Флаги (3 бита)	Смещение фрагментов (13 бит)
Время жизни (8 бит)	Протокол (8 бит)	Контрольная сумма заголовка (16 бит)	
IP-адрес источника (32 бита)			
IP-адрес приемника (32 бита)			
Параметры IP (может быть пустым)		Заполнение	
Данные датаграммы IP (до 65535 байт)			

IP-адрес

- Уникально идентифицирует рабочую станцию (сетевой интерфейс) в глобальном масштабе
- Длина адреса 32 бита (всего 4.394.967.296 адресов)
- IP v.4, IP v.6
- Имеет иерархическую структуру

Структура IP-адресов

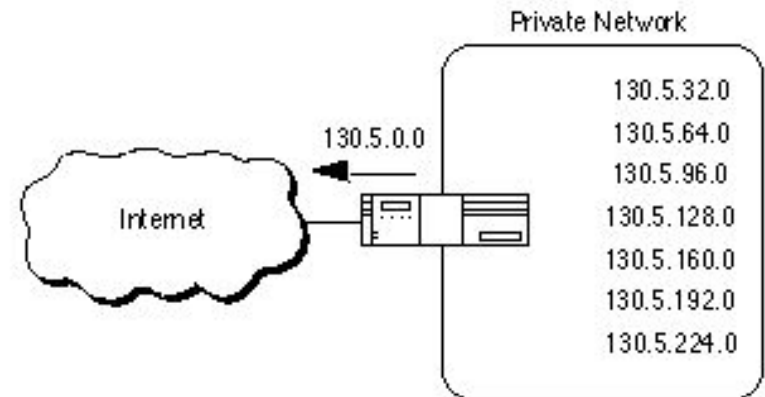
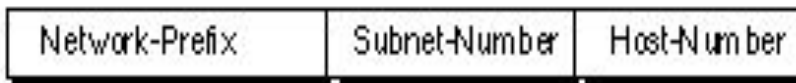
	0	8	16	24	31
Класс А	0	номер сети	номер узла		
Класс В	10	номер сети		номер узла	
Класс С	110	номер сети		номер узла	
Класс D	1110	групповой адрес			
Класс E	11110	зарезервировано			

Подсети

Two-Level Classful Hierarchy



Three-Level Subnet Hierarchy



Адресная иерархия при организации подсетей

- Не нужно запрашивать ещё один сетевой номер, прежде чем установить новую сеть в организации.

Порты

Порты отправителя и получателя - двухбайтовые поля. Имеют значения от 0 до 65536.

Идентифицируют приложения, данные которых переносит данный пакет протокола транспортного уровня. Механизм введен для того, чтобы разные приложения, работающие на одном узле сети, могли независимо друг от друга передавать свои данные.

Например, TELNET - 23, FTP - 21, SMTP - 25 (работают по TCP) и DNS - 53 (работает по UDP).

Протокол TCP

Протокол TCP обеспечивает гарантированную доставку с установлением соединений в виде байтовых потоков.

Используется в тех случаях, когда требуется надежная доставка сообщений, освобождает прикладные процессы от необходимости использовать таймауты и повторные передачи для обеспечения надежности. Прикладными процессами, использующими TCP, являются FTP, TELNET и многие другие.

Реализация TCP требует большой производительности процессора и большой пропускной способности сети. Внутренняя структура модуля TCP гораздо сложнее структуры модуля UDP.

Протокол UDP

Протокол UDP - User Datagram Protocol

Предоставляет прикладным процессам транспортные услуги. Обеспечивает ненадежную доставку датаграмм и не поддерживает соединений из конца в конец. К данным добавляются поля, одно из которых, поле "порт", обеспечивает мультиплексирование информации между разными прикладными процессами, а другое - "контрольная сумма" - позволяет определять целостность данных.

Протокол UDP

- Не требует подтверждения получения сообщений
- Не требует установления соединений

Переносит информацию о порте получателя и контрольную сумму.



Протокол RTP

- Производит нумерацию пакетов в потоке;
- Помечает пакеты временными метками;
- На приёмной стороне вычисляется средняя задержка;
- Осуществляет индикацию типа полезной нагрузки;
- Идентифицирует участников.

Протокол RTSP

- Обеспечение обратной связи для контроля качества при отправке данных
- Предоставляет «cname» для идентификации участников сессии
- Позволяет определять количество участников сессии
- Передача минимальной управляющей информации

Пакеты RTSP

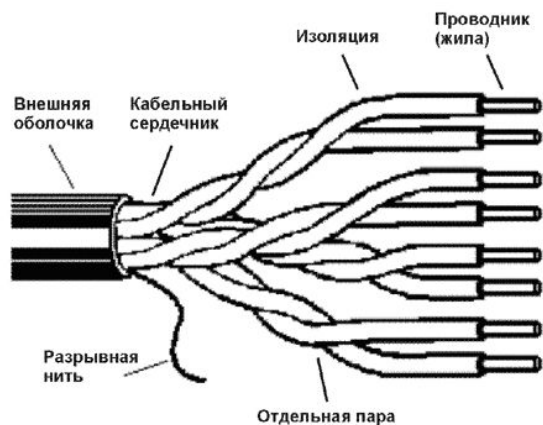
- **sr**: Отчет отправителя. Для статистики приема и передачи участников, которые являются активными отправителями
- **rr**: Отчет получателя. Для получения статистики от участников, которые не являются активными отправителями
- **sdes**: Элементы описания источника, включая `sname`
- **bye**: Отмечает прекращение участия в группе
- **app**: Специфические функции приложения

Физический уровень ТСП/IP

Физический уровень

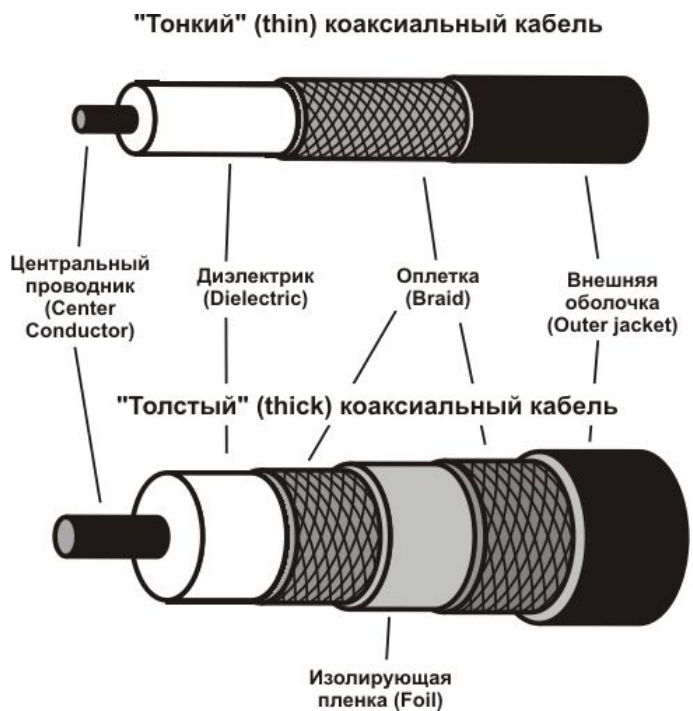
- нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому.
- Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п. Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: V.35, RS-232, RS-485, RJ-11, RJ-45, разъемы AUI и BNC.
- Протоколы физического уровня: IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi, Ether loop, GSM Um radio interface, ITU и ITU-T, TransferJet, ARINC 818, G.hn/G.9960.

Витая пара



- вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой.
- Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитные помехи одинаково влияют на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара — один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet, Arcnet и Token ring. В настоящее время, благодаря своей дешевизне и лёгкости в монтаже, является самым распространённым решением для построения проводных (кабельных) локальных сетей.

Коаксиальный кабель



- электрический кабель, состоящий из расположенных соосно центрального проводника и экрана. Обычно служит для передачи высокочастотных сигналов. Изобретён и запатентован в 1880 году британским физиком Оливером Хевисайдом.

Оптический кабель. Волоконно-оптическая связь



- ид проводной электросвязи, использующий в качестве носителя информационного сигнала электромагнитное излучение оптического (ближнего инфракрасного) диапазона, а в качестве направляющих систем — волоконно-оптические кабели. Благодаря высокой несущей частоте и широким возможностям мультиплексирования, пропускная способность волоконно-оптических линий многократно превышает пропускную способность всех других систем связи и может измеряться терабитами в секунду. Малое затухание света в оптическом волокне позволяет применять волоконно-оптическую связь на значительных расстояниях без использования усилителей. Волоконно-оптическая связь свободна от электромагнитных помех и труднодоступна для несанкционированного использования — незаметно перехватить сигнал, передаваемый по оптическому кабелю, технически крайне сложно.

Технологии передачи данных

Технологии передачи данных

- «ДиалАп» - модемные соединения
- xDSL – соединение поверх ТфОП
- PON\FTTx – оптика как «последняя миля»
- Ethernet – локальная сеть как «последняя миля»
- Беспроводной доступ – WiMax, 3G\4G (LTE)

xDSL

- семейство технологий, позволяющих значительно повысить пропускную способность абонентской линии телефонной сети общего пользования путём использования эффективных линейных кодов и адаптивных методов коррекции искажений линии на основе современных достижений микроэлектроники и методов цифровой обработки сигнала.

xDSL

- К основным типам xDSL относятся ADSL, HDSL, IDSL, MSDSL, PDSL, RADSL, SDSL, SHDSL, UADSL, VDSL.
- Все эти технологии обеспечивают высокоскоростной цифровой доступ по абонентской телефонной линии.
- Некоторые технологии xDSL являются оригинальными разработками, другие представляют собой просто теоретические модели, в то время как третьи уже стали широко используемыми стандартами.
- Основным различием данных технологий являются методы модуляции, используемые для кодирования данных.

xDSL

Технология DSL	Максимальная скорость (прием/передача)	Максимальное расстояние	Количество телефонных пар	Основное применение
<u>ADSL</u>	24 Мбит/с / 3,5 Мбит/с	5,5 км	1	Доступ в <u>Интернет</u> , голос, видео, <u>HDTV</u> (ADSL2+)
<u>IDSL</u>	144 кбит/с	5,5 км	1	<u>Передача данных</u>
<u>HDSL</u>	2 Мбит/с	4,5 км	1,2	Объединение сетей, услуги <u>E1</u>
<u>SDSL</u>	2 Мбит/с	3 км	1	Объединение сетей, услуги <u>E1</u>
<u>VDSL</u>	62 Мбит/с / 26 Мбит/с	1,3 км на макс. скорости	1	Объединение сетей, <u>HDTV</u>
<u>SHDSL</u>	2,32 Мбит/с	7,5 км	1	Объединение сетей
<u>UADSL</u>	1,5 Мбит/с / 384 кбит/с	3,5 км на макс. скорости	1	Доступ в <u>Интернет</u> , голос, видео

ADSL

- Передача данных по технологии ADSL реализуется через обычную аналоговую телефонную линию при помощи абонентского устройства — модема ADSL и мультиплексора доступа (*DSL Access Multiplexer, DSLAM*), находящегося на той АТС, к которой подключается телефонная линия пользователя, причём включается DSLAM до оборудования самой АТС. В результате между ними оказывается канал без каких-либо присущих телефонной сети ограничений. DSLAM мультиплексирует множество абонентских линий DSL в одну высокоскоростную магистральную сеть.
- Также они могут подключаться к сети АТМ по каналам PVC (постоянный виртуальный канал, англ. *Permanent Virtual Circuit*) с провайдерами услуг Internet и другими сетями.
- Стоит заметить, что два ADSL-модема не смогут соединиться друг с другом, в отличие от обычных dial-up-модемов.

ADSL

- Технология ADSL представляет собой вариант DSL, в котором доступная полоса пропускания канала распределена между исходящим и входящим трафиком несимметрично — для большинства пользователей входящий трафик значительно более существенен, чем исходящий, поэтому предоставление для него большей части полосы пропускания вполне оправдано (исключениями из правила являются пиринговые сети, видеозвонки и электронная почта, где объём и скорость исходящего трафика бывают важны).
- Обычная телефонная линия использует для передачи голоса полосу частот 0,3...3,4 кГц. Чтобы не мешать использованию телефонной сети по её прямому назначению, в ADSL нижняя граница диапазона частот находится на уровне 26 кГц. Верхняя же граница, исходя из требований к скорости передачи данных и возможностей телефонного кабеля, составляет 1,1 МГц.
- Эта полоса пропускания делится на две части — частоты от 26 кГц до 138 кГц отведены исходящему потоку данных, а частоты от 138 кГц до 1,1 МГц — входящему.
- Полоса частот от 26 кГц до 1,1 МГц была выбрана не случайно. В этом диапазоне коэффициент затухания почти не зависит от частоты.

Часть 3.

Стек TCP/IP для передачи мультимедийного трафика реального времени

IP телефония

Телефония – услуга связи, позволяющая передавать голосовые сообщения.

IP телефония – услуга связи, позволяющая передавать голосовые сообщения в цифровом виде с использованием протокола IP.

(Более эффективное использование сетевых ресурсов)

Применение кодеков для передачи речи в IP среде

- Разрезают непрерывную речь на порции
- Позволяют сжимать передаваемые порции информации на основе предсказаний

Передача данных по IP-сетям в реальном времени

- Необходимо обеспечить минимальное время задержки пакетов и небольшое значение джиттера;
- Необходимо контролировать последовательность пакетов;
- Необходимо контролировать время задержки;
- Необходимо контролировать потери пакетов.

Часть 4

Обеспечение гарантированного качества для
мультимедийного трафика

Мультимедийный трафик

- Голос
- Видео
- Данные

Качество услуг

Качество

Субъективно

Экспертная оценка:
Отлично
Хорошо
Удовлетворительно

Объективно

Нормы на услуги:
Тзадержки мах
Тджиттера мах
% допустимых потерь

QoS для VoIP

- QoS

- «Набор требований к поведению сети» (ITU-T);
- Вероятность того, что сеть связи соответствует заданному соглашению о трафике;
- Концепция улучшения качества предоставляемых услуг

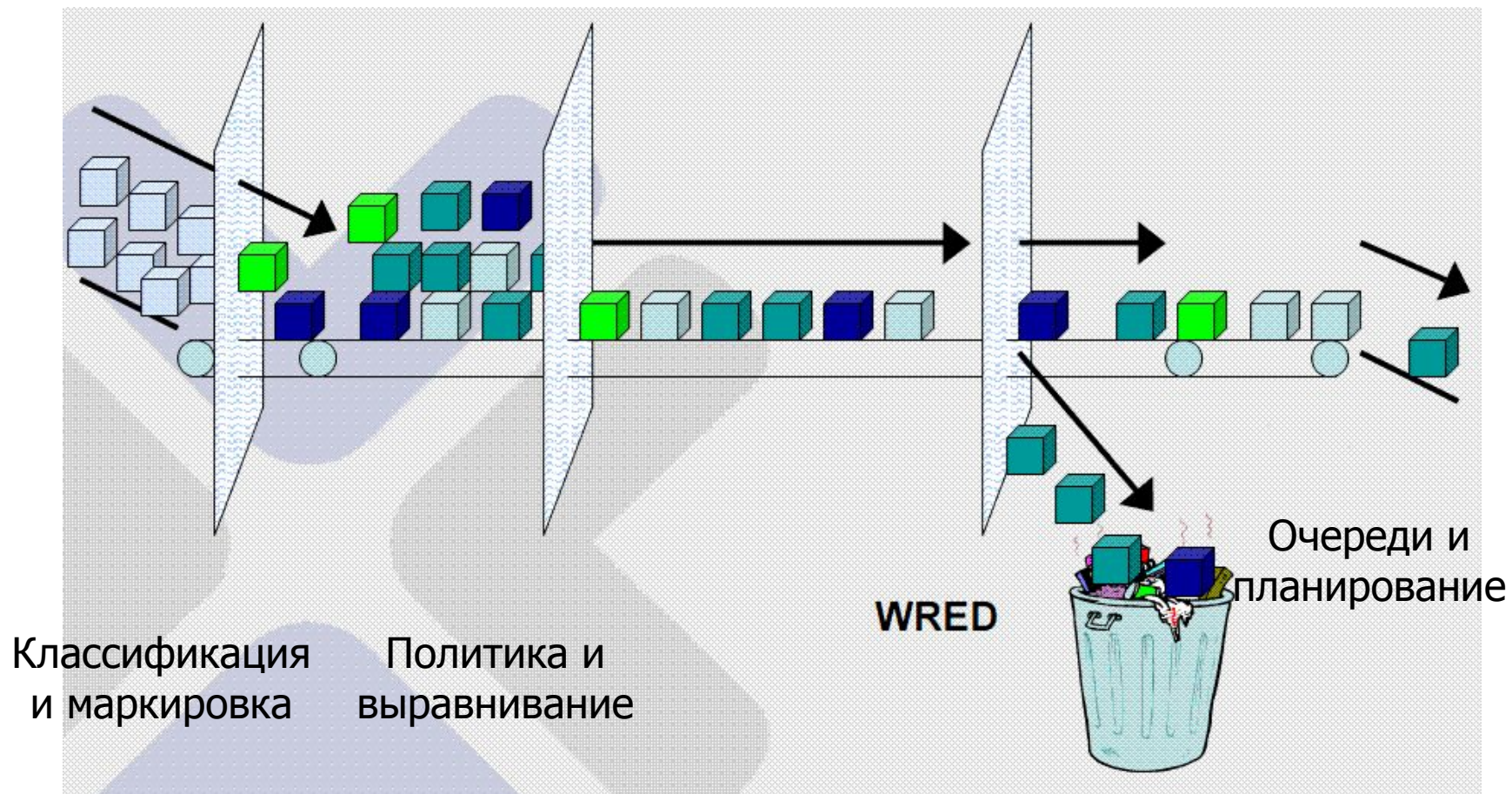
- VoIP

- Концепция передачи голосовых сообщений через сеть с пакетной коммутацией на базе протокола IP

Нормирование качества

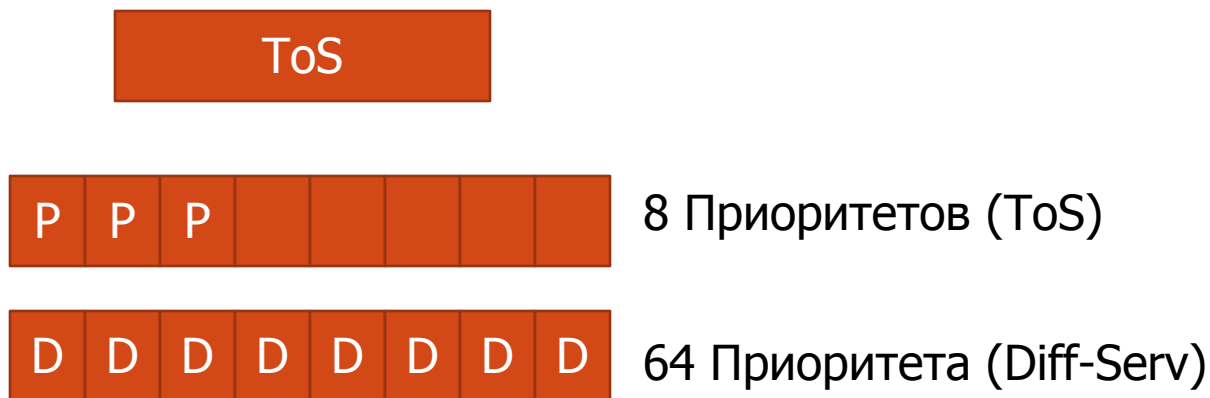
Показатели качества передачи речи		Классы качества услуги			
		Лучшее	Высокое	Среднее	Низкое
Время установления соединения	прямая IP-адресация	< 1.5 сек	< 4 сек	< 7 сек	—
	перевод номера E.164 в IP-адрес	< 2 сек	< 5 сек	< 10 сек	—
	перевод номера E.164 в IP-адрес через расчётную организацию	< 3 сек	< 8 сек	< 15 сек	—
	перевод имени e-mail в IP-адрес	< 4 сек	< 13 сек	< 25 сек	—
Сквозные задержки	по стандарту ETSI TS101329	< 150 мс	< 250 мс	< 350 мс	< 450 мс
	по рекомендации ITU-T G.114	< 150 мс	< 260 мс	< 400 мс	> 400 мс
Качество воспринимаемой речи	ETSI	Не хуже G.711	Не хуже G.726 для 32 кбит/сек	Не хуже GSM-FR	С максимальными усилиями
	Баллы MOS	> 4.5	4.0 — 4.5	3.5 — 4.0	3.5 — 3.0

Операции QoS



Классификация и маркировка

- Заполнение битов в заголовках пакетов и кадров.
 - Заполнение поля ToS (Type of Service) в заголовке IP пакета



- Технология дифференцированного обслуживания разнотипного трафика (механизмы Diff-Serv)
- Технология резервирования ресурсов на основе протокола RSVP
- Технология многопротокольной коммутации по меткам (MPLS)

Политика и выравнивание

- Политика и выравнивание – определяют алгоритм сглаживания пульсации трафика и контроль заказанной полосы пропускания
 - Leaky Bucket
 - Token Bucket

Очереди и планирование

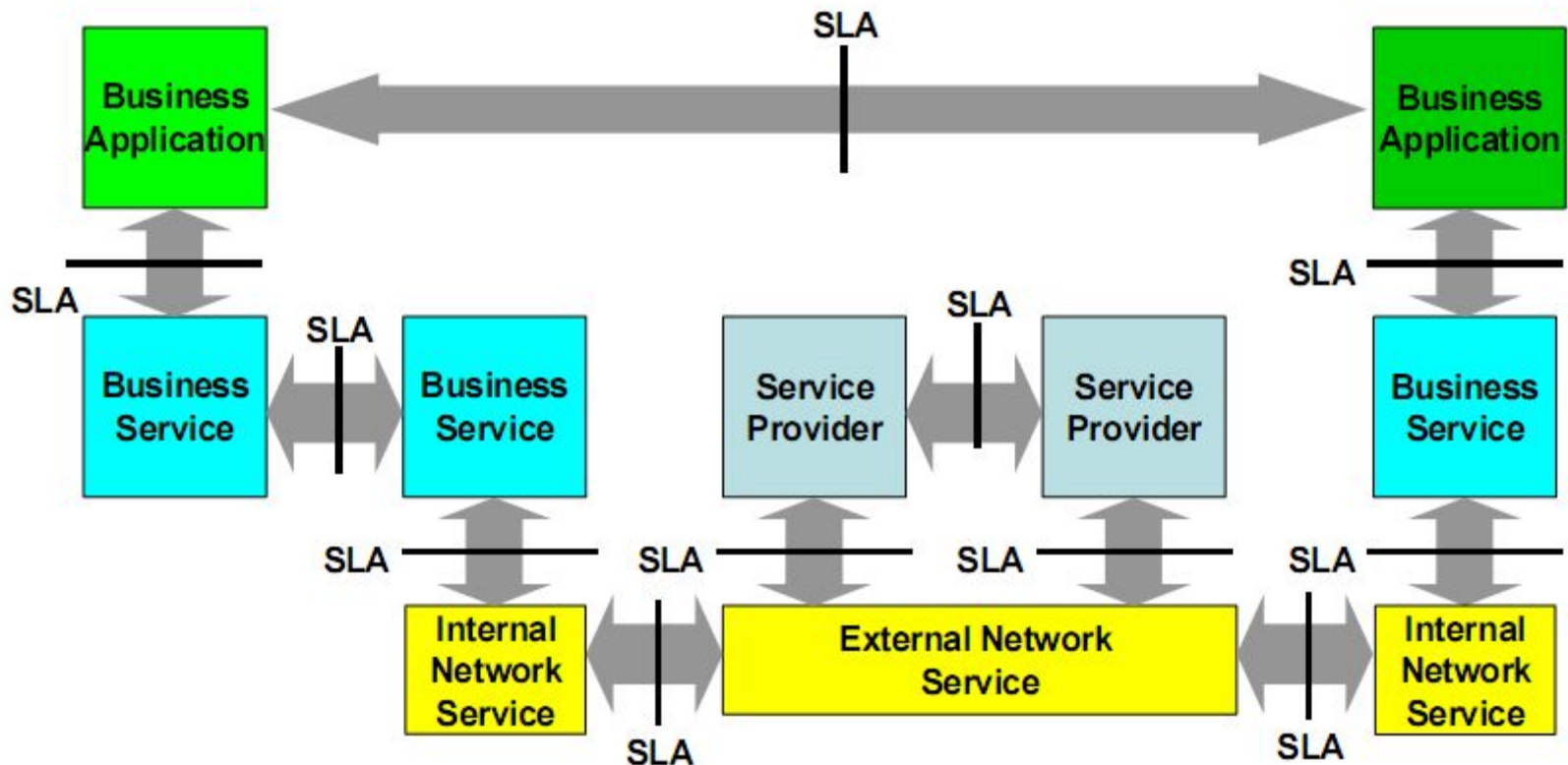
- FIFO
- Очередь с приоритетами
- Class Based Queuing (CBQ)
- Взвешенные очереди

Соглашение о качестве обслуживания, SLA

SLA (Service Level Agreement)

- SLA – это часть договора между двумя сторонами, в которой нормируется качество предоставляемых услуг.
- Состав SLA:
 - Определение услуги
 - Описание процедуры измерений и отчетов качества услуг
 - Нормирование времени реализации обращений
 - Обязанности стороны, нарушающей условия договора

Участники SLA



Контроль SLA

- Сбор информации
- Учет требований SLA
- Обработка информации

Контроль SLA

