Компьютерные сети

К.т.н., доцент кафедры ИУС
Феликс Васильевич Филиппов
9000096@mail.ru

Компьютерные сети

Особенности LAN, MAN, GAN и HAN
Стандарты и архитектура сети
Эталонные модели
Среды передачи информации
Кодирование информации в сетях
Кадры и пакеты
Адресация
Тенденции развития сетей
Службы и протоколы Интернета
WEB - программирование
Безопасность в сетях

Сети

Зона доступа и охвата

- LAN - Local Area Network
- MAN - Metropolitan Area Network
- GAN - Global Area Network
- HAN - Home Area Network

Компьютерные сети

Зона доступа и охвата (уточнение)

Расстояние между процессорами	Где процессоры расположены	Что это?
1 м	На одном кв. метре	Персональная сеть
10 м	Комната	Локальная сеть
100 м	Здание	
1 км	Кампус	
10 км	Город	Муниципальная сеть
100 км	Страна	Глобальная сеть
1000 км	Континент	
10000 км	Планета	Интернет

Локальные сети

- **соединяют близко расположенные компьютеры**
- **связывает небольшое количество компьютеров**

- позволяют пользователям не замечать связи и объединяются, по сути, в один виртуальный компьютер
- скорость обмена 1-10 Мбит/с
  100 Мбит/с
  1000 Мбит/с и выше
- возможность работы с большими нагрузками, то есть с большой интенсивностью обмена (с большим трафиком)

Назначение локальных сетей

Экономия во всем

- Распределение ресурсов (**Resource Sharing**)
- Распределение данных (**Data Sharing**)
- Распределение программ (**Software Sharing**)
- Электронная почта (**Electronic Mail**)

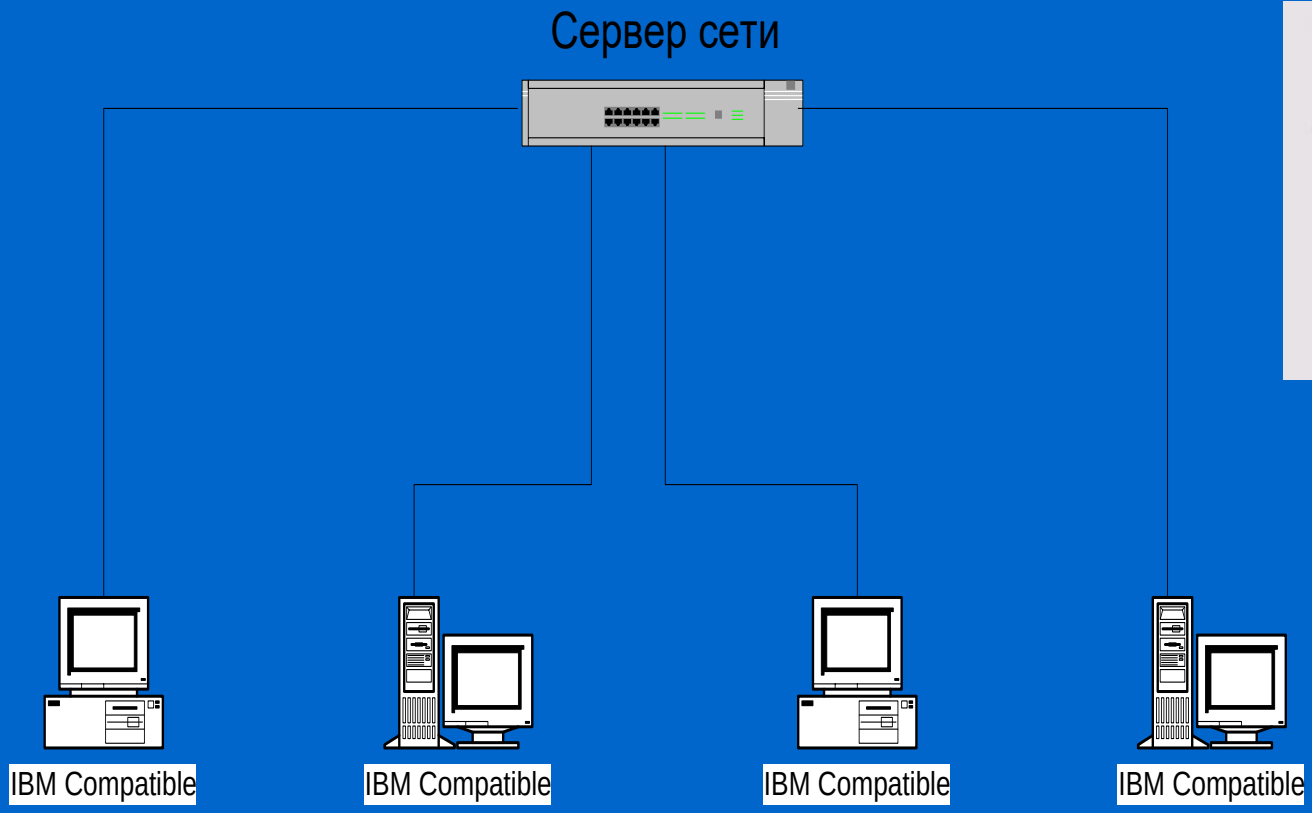
Администрирование локальной сети

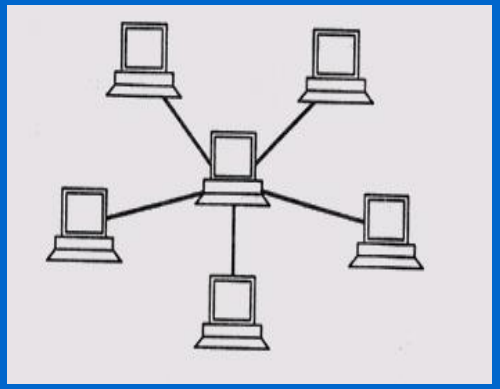
Задачи администратора

- Надежное функционирование (**Reliability**)
- Защита от сбоев электропитания (**UPS**)
- Защита данных (**Disk Arrays**)
- Разграничение прав доступа (**Privileges**)

Топология локальной сети

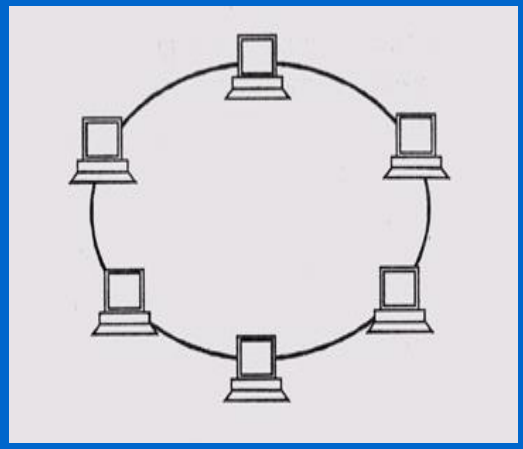
Звезда (Star)

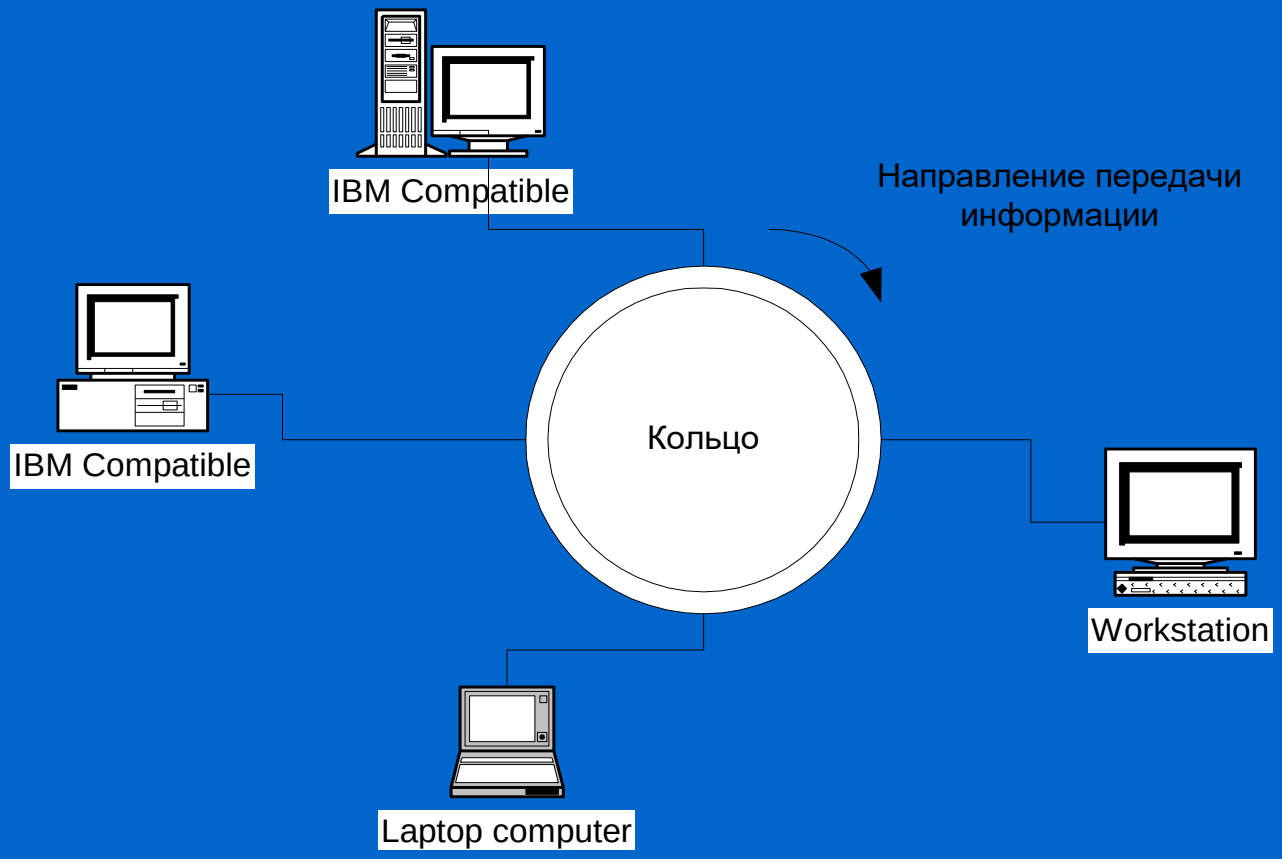




Топология локальной сети

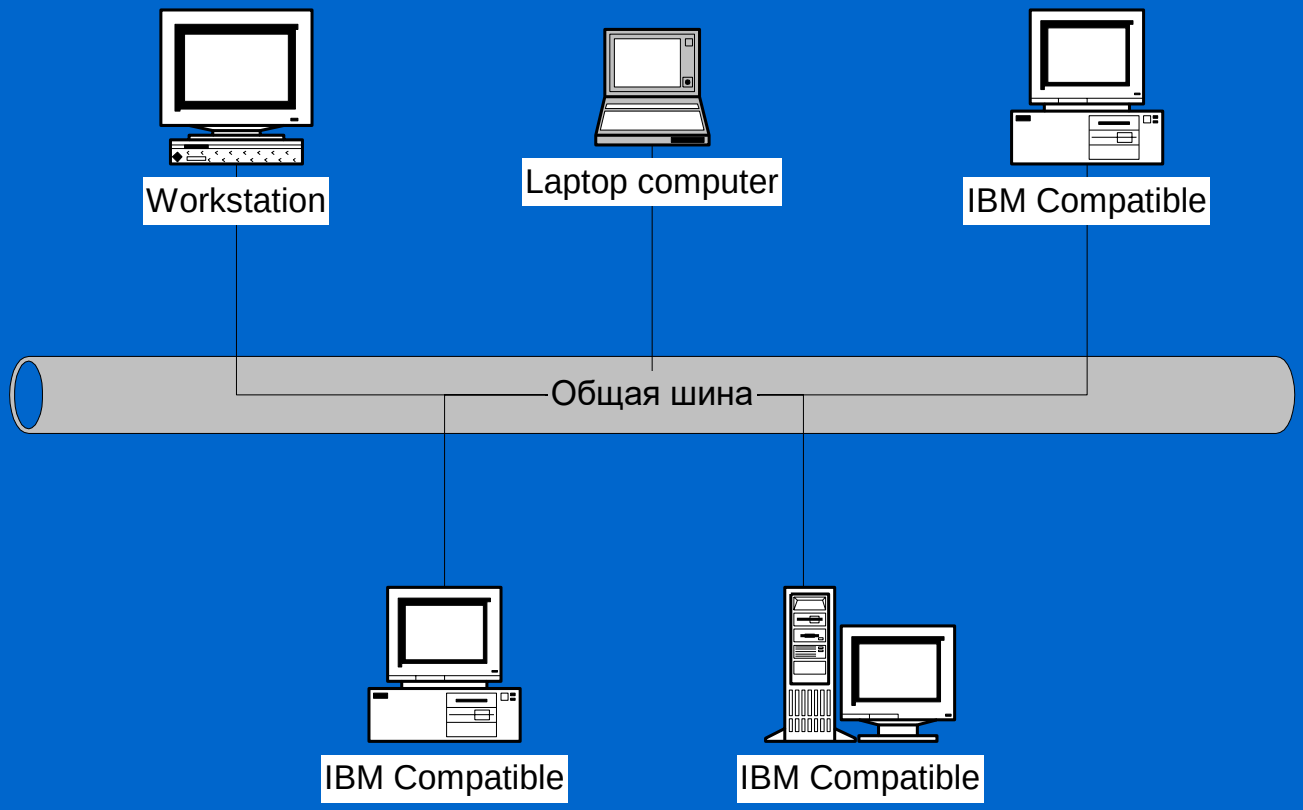
Кольцо (Ring)

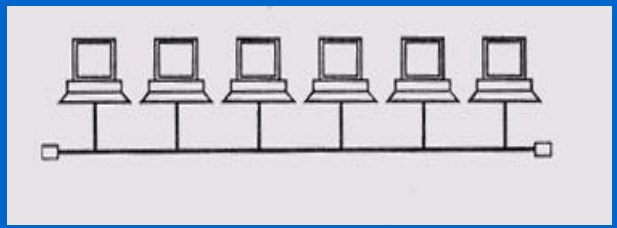




Топология локальной сети

Общая шина (Bus)

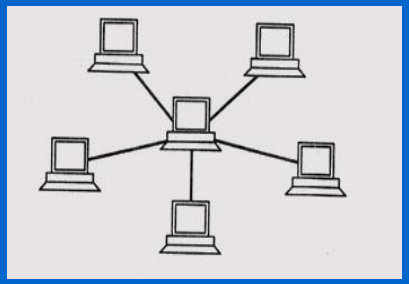




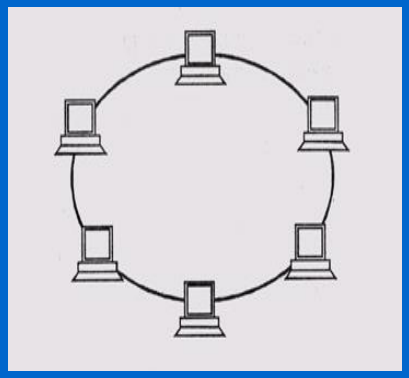
Сравнение классических топологий ЛС

Arcnet, Token Ring, Ethernet

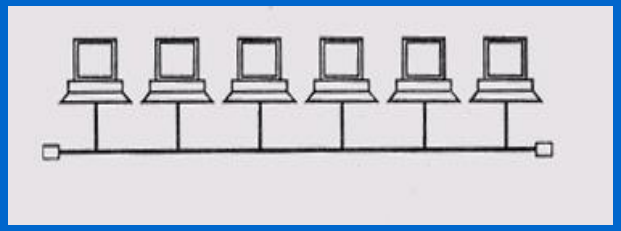
- Звезда (Star)



- Кольцо (Ring)



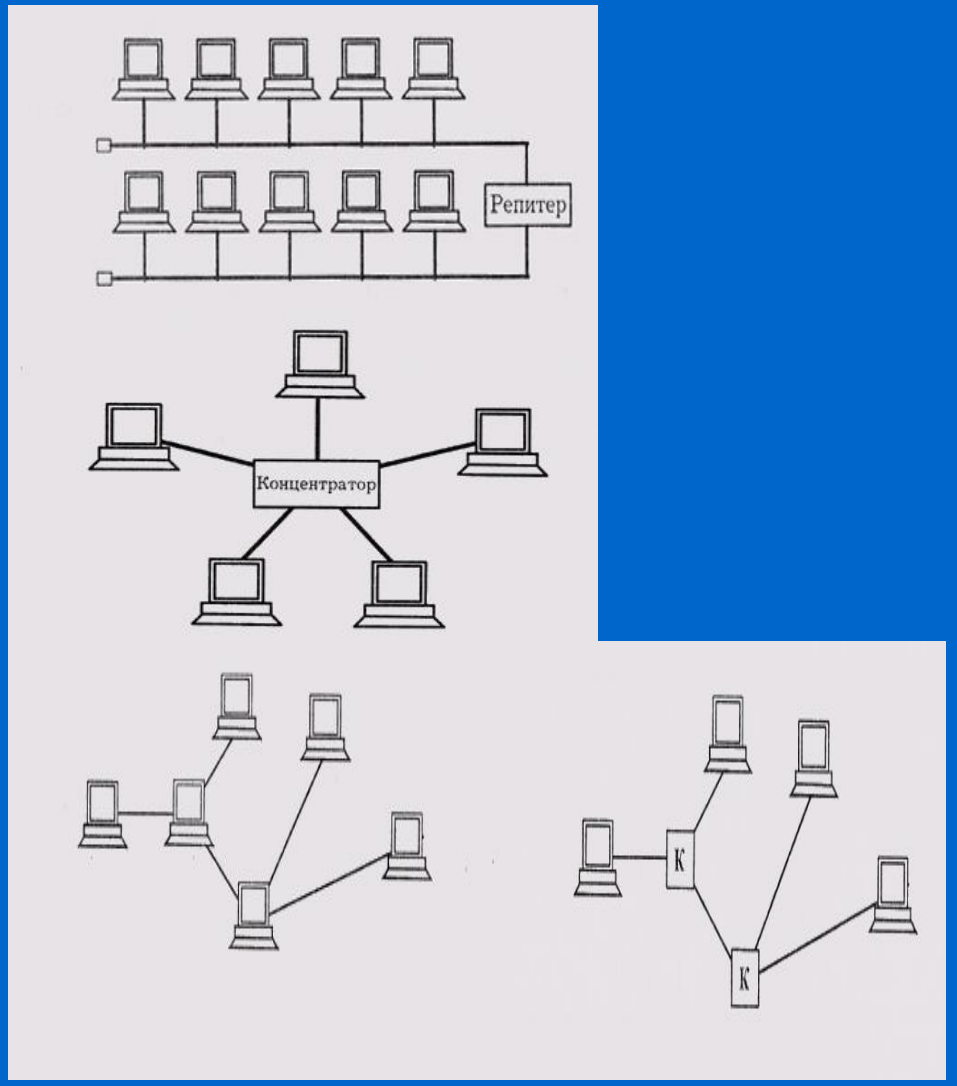
- Общая шина (Bus)



Произвольные топологии ЛС

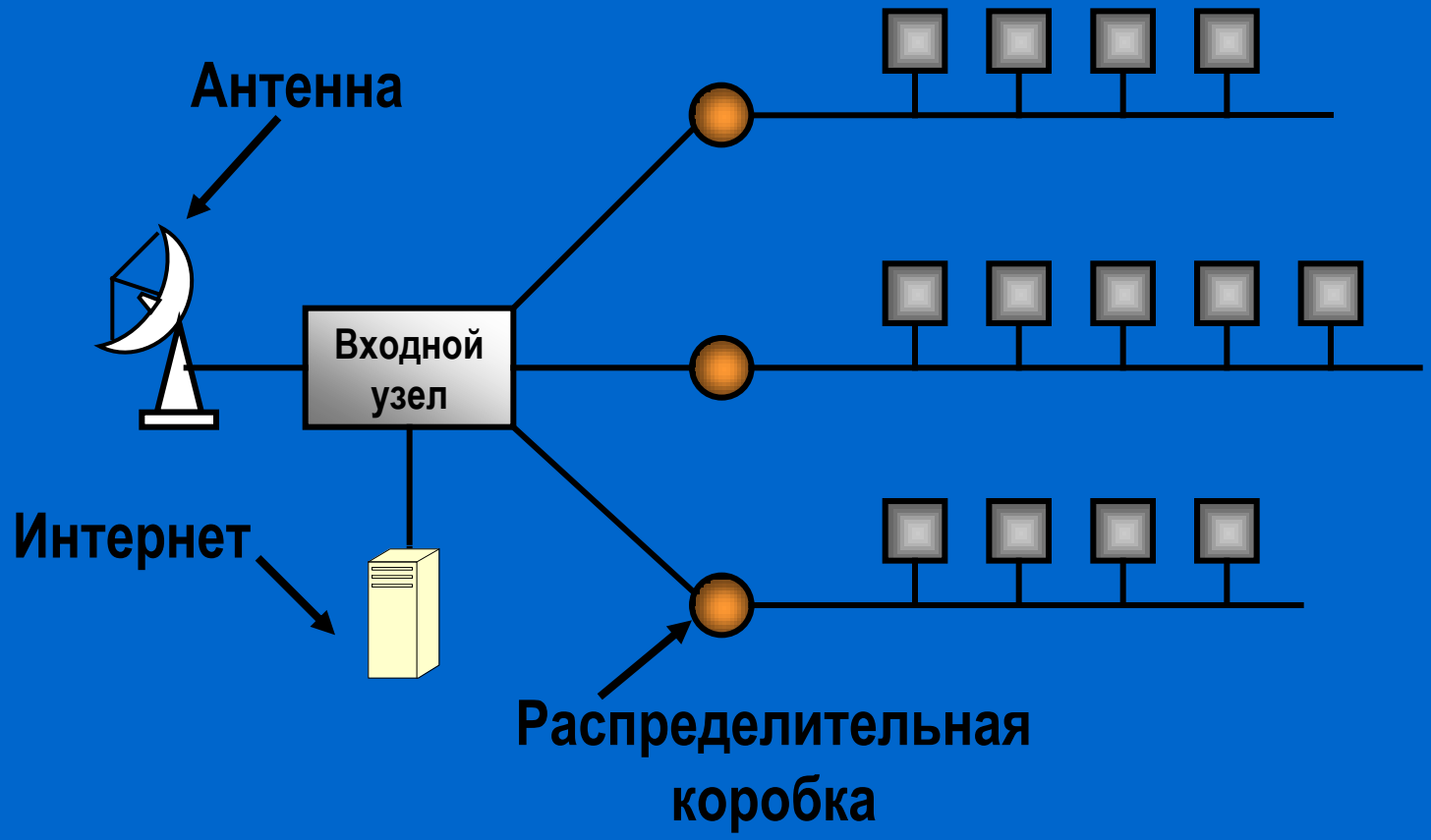
Использование повторителей и концентраторов

- Повторитель (Repeater)
- Концентратор (Hub)
  Пассивная звезда
- Активное дерево
  Пассивное дерево (Hub)



Муниципальные сети

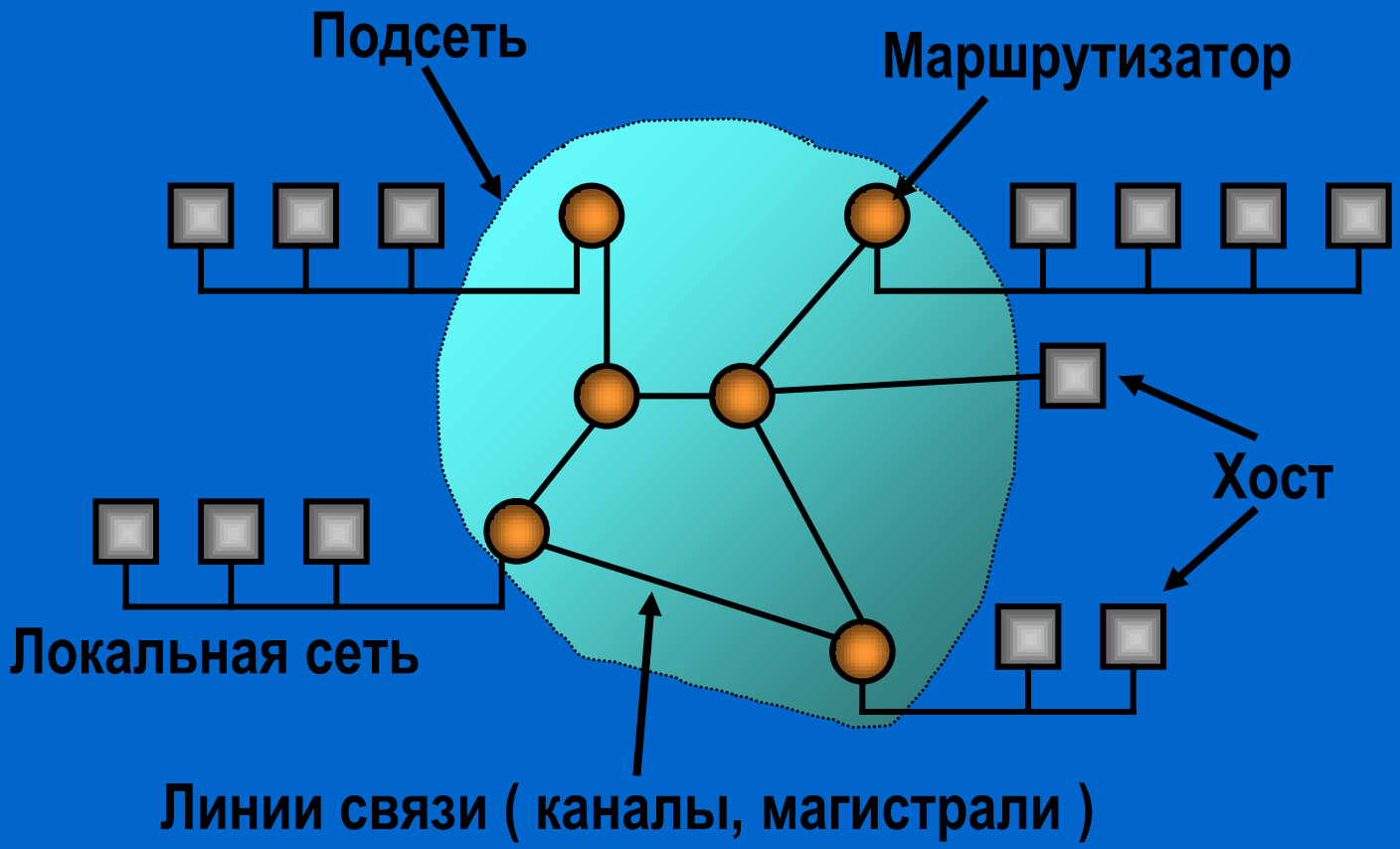
Эфирные, кабельные



Глобальные сети

Хосты, каналы, маршрутизаторы

Хост – собственность клиента для выполнения приложений (прикладной аспект сети)
Подсеть – набор линий связи и маршрутизаторов (коммуникативный аспект сети)



Особенности глобальных сетей

Два основных понятия:	адрес и протокол
Два основных протокола:	IP (Internet Protocol)
	TCP (Transmission Control Protocol)

TCP / IP

Передача информации

TCP – разбивает файл на части, нумерует их и передает протоколу IP

IP – к каждой части добавляет IP-адрес назначения и IP-пакеты отправляет в сеть

Распространение информации

В сети пакеты могут пересылаться разными путями и по разным средам.

Прием информации

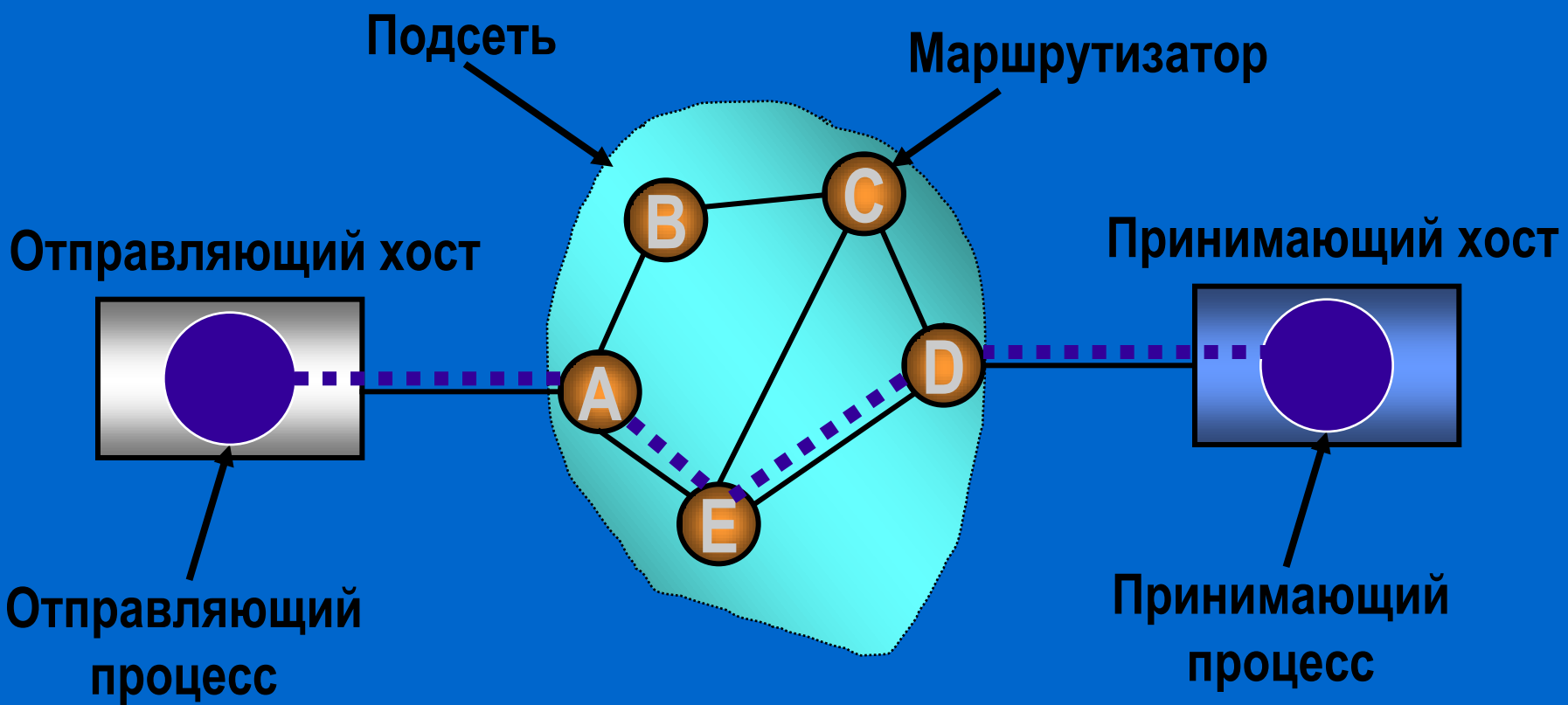
IP – пакеты принимаются из сети, убираются адреса и передаются протоколу TCP

TCP – сортирует части по номерам и собирает файл из частей

Особенности глобальных сетей

Потоки пакетов

Маршрутизатор E принял решение переслать пакеты в D, а не в C



Особенности глобальных сетей

Сервисы (службы) и протоколы

- **Электронная почта**
  SMTP – Simple Mail Transfer Protocol (Простой протокол пересылки почты)
  POP3 – Post Office Protocol (Протокол почтового офиса)

- **Хранилища файлов**
  FTP – File Transfer Protocol (Протокол передачи файлов)

- **Сервис WWW (World Wide Web)**
  HTTP – Hyper Text Transfer Protocol (Протокол передачи гипертекста)

Домашние сети

Узлы и требования

- Компьютеры (настольные, ноутбуки, PDA)
- Приборы для развлечений (TV, DVD, видеокамеры, аудиосистемы, MP3-проигрыватели)
- Телекоммуникации (различные телефоны, факсы)
- Бытовые приборы (СВЧ-печи, холодильники, отопительные приборы, кондиционеры, системы освещения)
- Измерительные приборы (счетчики, датчики пожарной сигнализации)
- Системы охранной сигнализации

- Простота
- Мощная защита от дурака
- Низкая цена
- Раз мультимедиа – высокое быстродействие
- Должны обладать свойством наращиваемости
- Защита информации

Компьютерные сети

Стандарты

Организация	Разработки
ISO – International Standards Organization Международная Организация по Стандартизации	Семиуровневая эталонная модель **OSI**
DoD - Department of Defense Министерство обороны США	Стек транспортных протоколов **TCP / IP**
ITU - International Telecommunications Unit Международный союз электросвязи в рамках ООН	Стандарты на сети **X.25**, frame relay и **ISDN**
IEEE - Institute of Electrical and Electronics Engineers Институт инженеров по электротехнике и электронике	Стандарты **802**
EIA - Electronic Industries Association Ассоциация электронной промышленности (США)	Интерфейс последовательных линий **RS-232C**
ANSI - American National Standards Institute Американский национальный институт стандартов	Архитектура локальных сетей крупных ЭВМ
ISOC - Internet Society Сообщество, занимающееся развитием сети Internet	Стандарты работы **Internet** **RFC - Request For Comments** – Запрос на комментарии

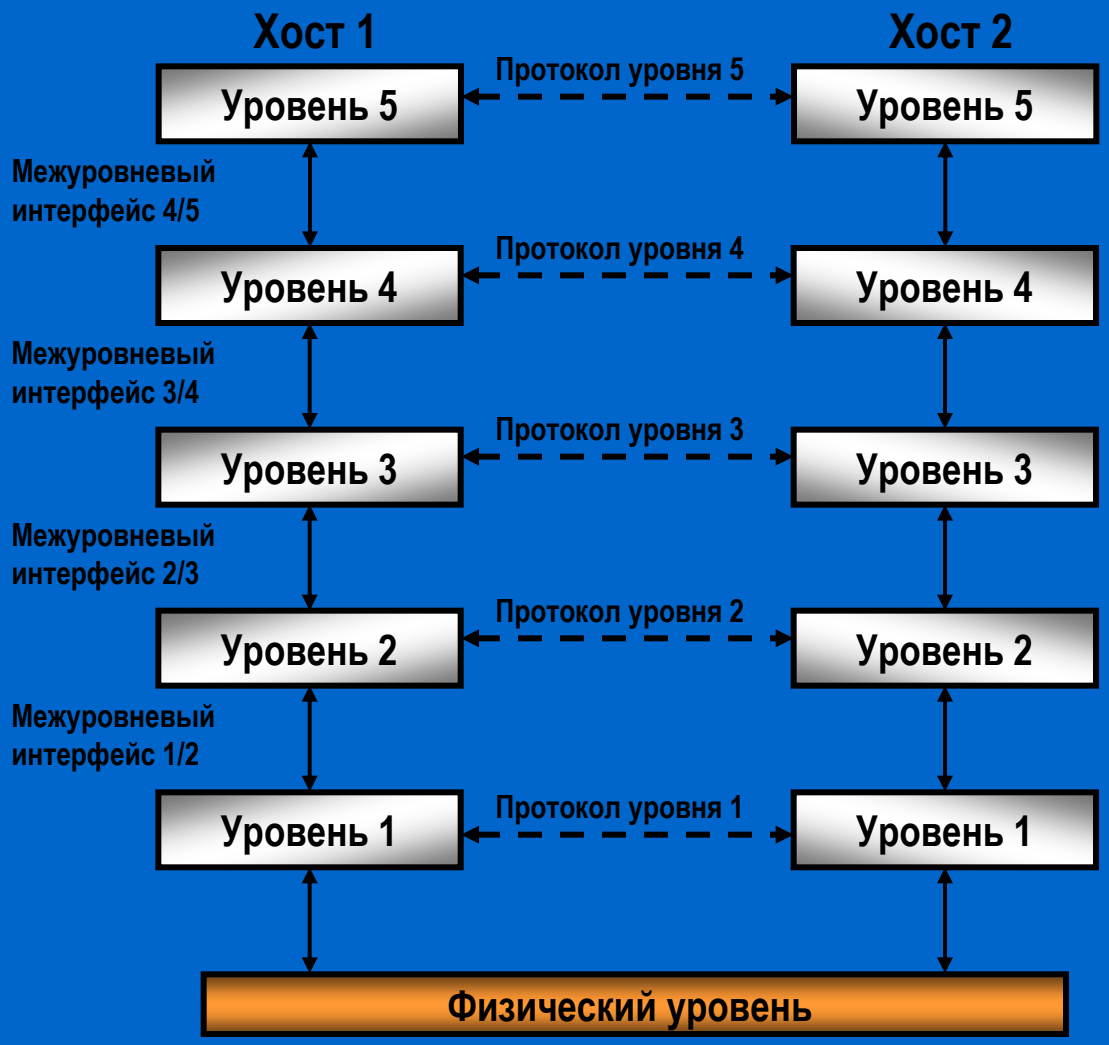
Стандарты модели

IEEE Project 802

Номер	Тема разработок
802.1	Общее представление и архитектура сети.
802.2	Управление логической связью.
802.3	Ethernet
802.4	Локальная сеть с топологией «шина» и маркерным доступом.
802.5	Локальная сеть с топологией «кольцо» и маркерным доступом.
802.6	Городская сеть (Metropolitan Area Network, MAN).
802.7	Широковещательная технология.
802.8	Оптоволоконная технология.
802.9	Интегрированные сети с возможностью передачи речи и данных.
802.10	Виртуальные локальные сети и защита информации.
802.11	Беспроводная сеть (WiFi – инфракрасный + 2,4 Ггц FHSS и DSSS).
802.12	Локальная сеть с централизованным управлением доступом по приоритетам запросов.
802.13	
802.14	Кабельные модемы.
802.15	Персональные сети (Bluetooth) – Гаральд Синий Зуб 949-981 великий король викингов piconet – scatternet
802.16	Широкополосные беспроводные локальные сети
802.17	Гибкая технология пакетного кольца.

Архитектура сети

Иерархия уровней и протоколов



Набор:
уровни + протоколы =
архитектура сети

Список:
по одному протоколу на уровень –
стек протоколов

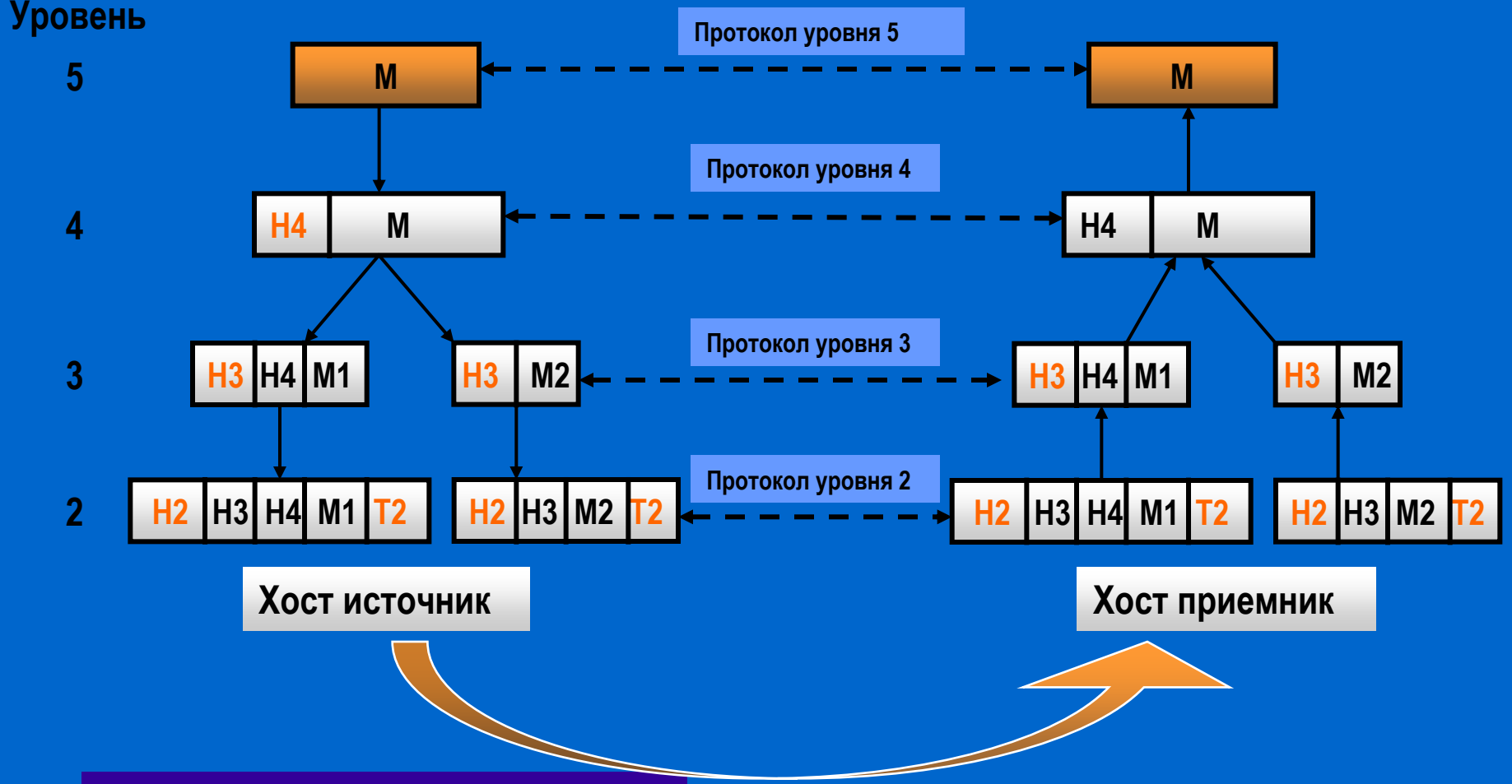
Реальное общение

Виртуальное общение

Архитектура сети

Назначение уровней и протоколов

Одноранговые процессы считают свое общение горизонтальным (SendToOtherSide и GetFromOtherSide). Абстракция одноранговых процессов является ключевой для проектирования сетей.



Архитектура сети

Разработка уровней

- Каждый уровень нуждается в механизме идентификации отправителей и получателей (адресация).
- Необходимо выработать правила переноса данных (в одном направлении, в любом направлении).
- Требуется обеспечить контроль ошибок передачи, т.е. договориться о коде и о процедуре повтора.
- Не все каналы сохраняют последовательность передачи пакетов – нужна нумерация и сортировка.
- Как организовать пересылку с медленной принимающей стороной? Требуется управление потоком.
- Неспособность всех процессов принимать сколь угодно длинные сообщения. Объединение – разбивка.
- Когда неудобно устанавливать отдельное соединение для каждой пары процессов – уплотнение каналов (мультиплексирование).
- Когда между отправителем и получателем несколько возможных путей – решается задача маршрутизации.

Архитектура сети

Надежные и ненадежные службы

Каждая служба характеризуется качеством обслуживания, некоторые службы являются надежными в том смысле, что они никогда не теряют данных.

Тип службы	Служба	Пример
С установлением соединения	Надежный поток сообщений	Последовательность страниц
	Надежный поток байт	Удаленная регистрация
	Надежное соединение	Цифровая голосовая связь
Без установления соединения	Ненадежная дейтаграмма	Рассылка рекламы электронной почтой
	Дейтаграмма с подтверждением	Заказные письма
	Запрос – ответ	Запрос к базе данных

Архитектура сети

Примитивы служб

Каждая служба (сервис) формально описывается набором примитивов или операций доступных пользователю для получения обслуживания.

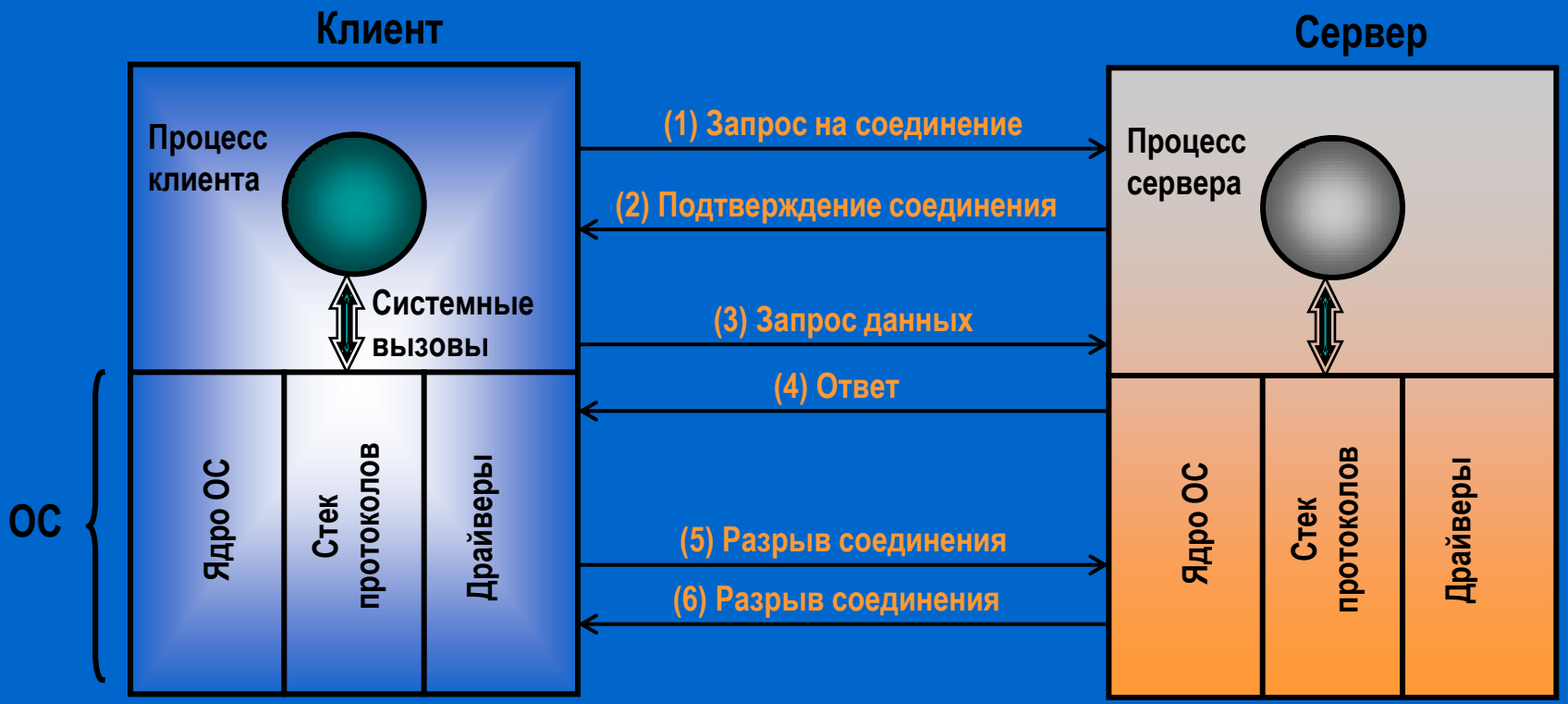
Примитив (системный вызов)	Оказываемое действие
LISTEN (ожидание)	Блок ожидает входящего соединения
CONNECT (соединение)	Установление соединения
RECEIVE (прием)	Блок ожидает входящего сообщения
SEND (отправка)	Отправка сообщения
DISCONNECT (разрыв)	Разрыв соединения

Пять сервисных примитивов, обеспечивающих передачу с установлением соединения

Архитектура сети

Пример использования примитивов

Простейшее взаимодействие клиента и сервера при передаче пакетов по сети с установлением соединения

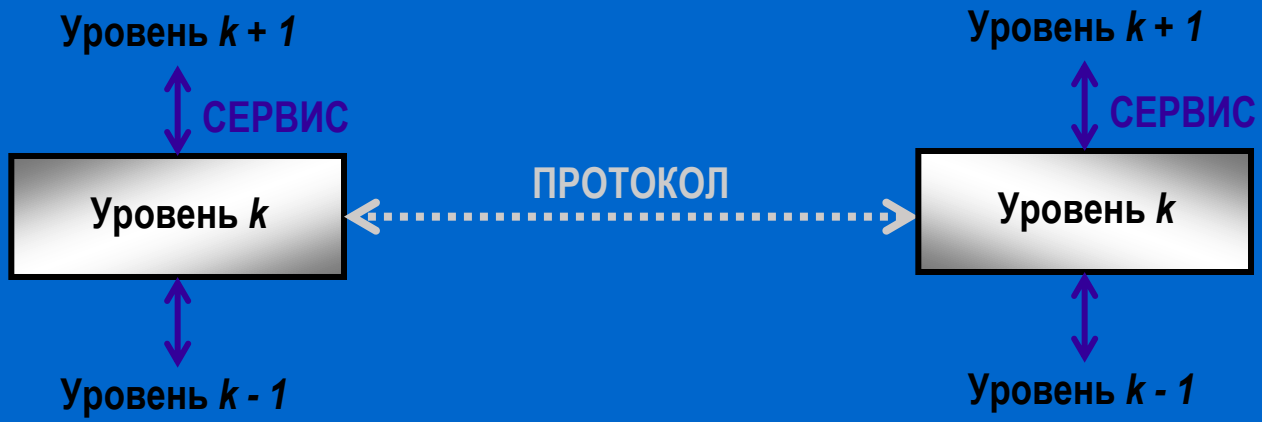


Архитектура сети

Службы (сервисы) и протоколы

СЛУЖБА (или СЕРВИС) – это набор примитивов (операций) , которые более низкий уровень предоставляет более высокому.

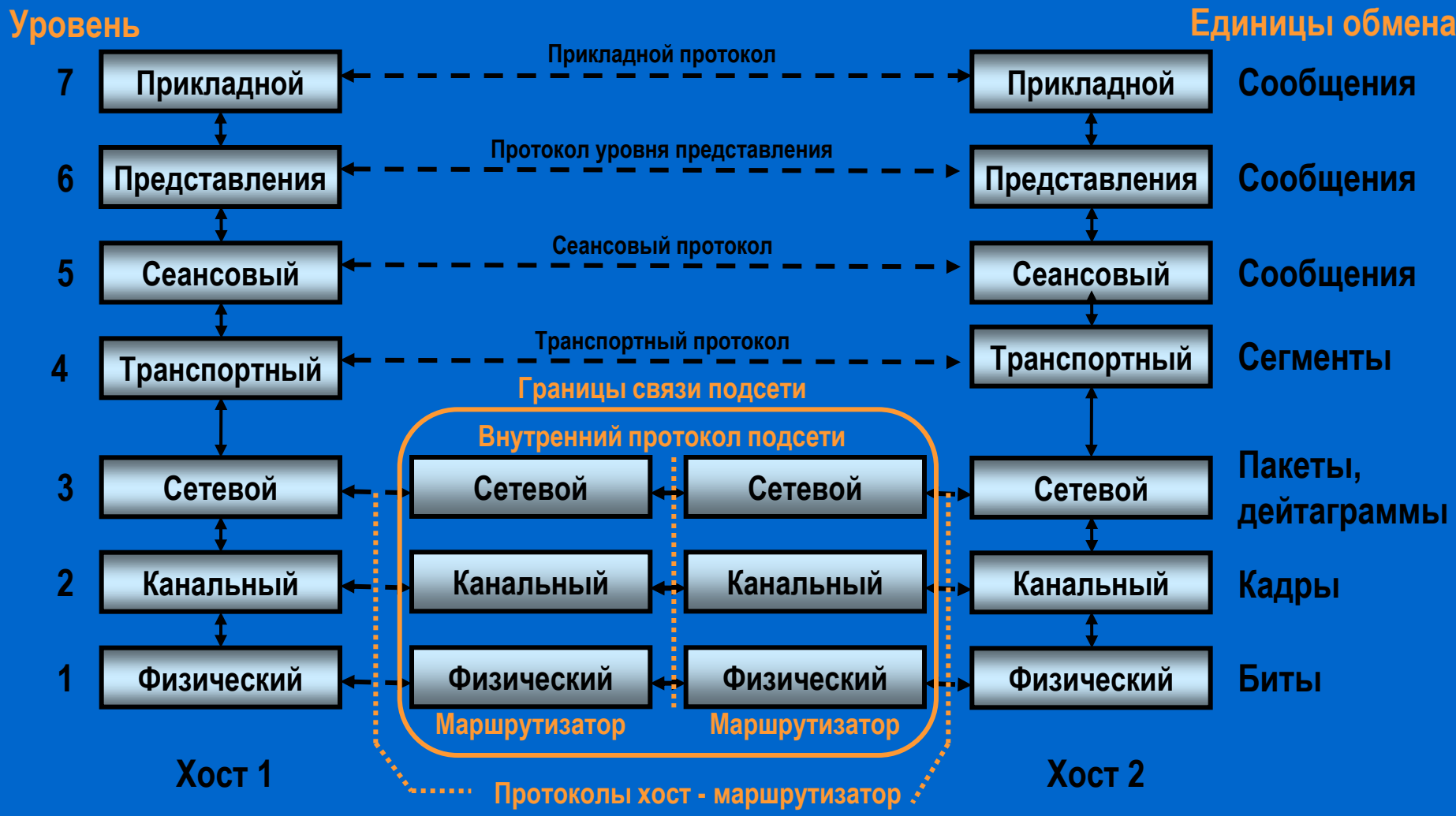
ПРОТОКОЛ – это набор правил, описывающих формат и назначение кадров, пакетов или сообщений, которыми обмениваются одноранговые сущности внутри уровня.



СЛУЖБЫ связаны с межуровневыми интерфейсами, а ПРОТОКОЛЫ – с пакетами, передающимися сущностями одного уровня, расположенными на разных машинах. СЛУЖБА – это объект, он определяет операции, которые могут с ним выполняться, но не описывает их реализацию. ПРОТОКОЛ – относится к реализации службы и не видим для пользователей службы.

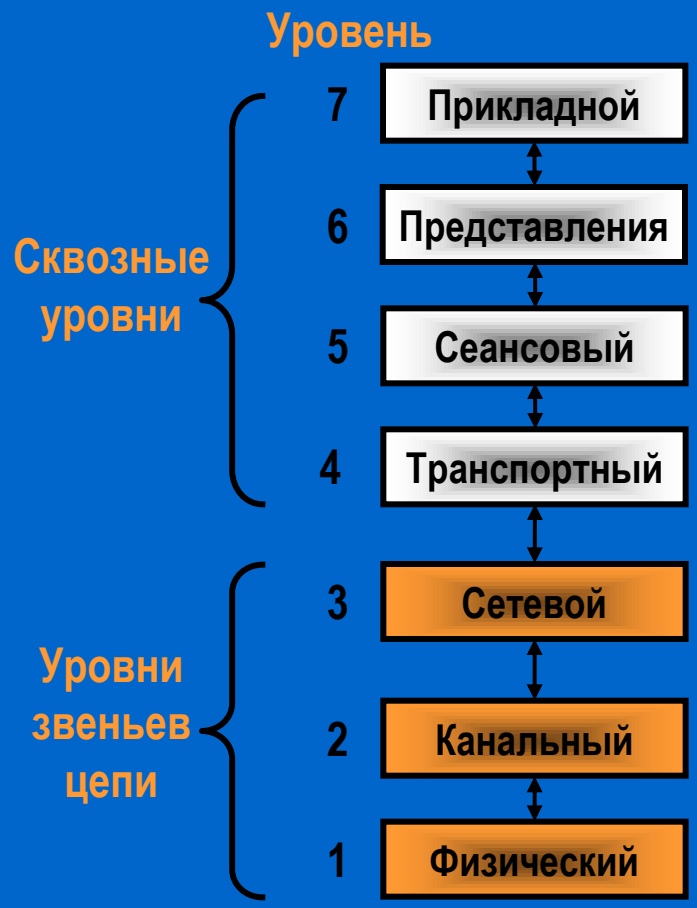
Эталонные модели

Эталонная модель OSI



Эталонные модели

Эталонная модель OSI



Open System Interconnection 1983, 1995

Содержит набор популярных протоколов необходимых пользователю. HTTP для WWW.

Занимается синтаксисом и семантикой сообщений. Преобразует форматы данных различных типов компьютеров.

Позволяет пользователям устанавливать сеансы связи. Разные сервисы – управление диалогом и синхронизация.

Сегментирует сообщения и гарантирует правильную доставку. Определяет тип сервиса при установке соединения.

Управляет операциями подсети – маршрутизация. Позволяет объединять разнородные сети.

Передача данных без ошибок – кадрами. Кадры данных передаются последовательно с кадрами подтверждения.

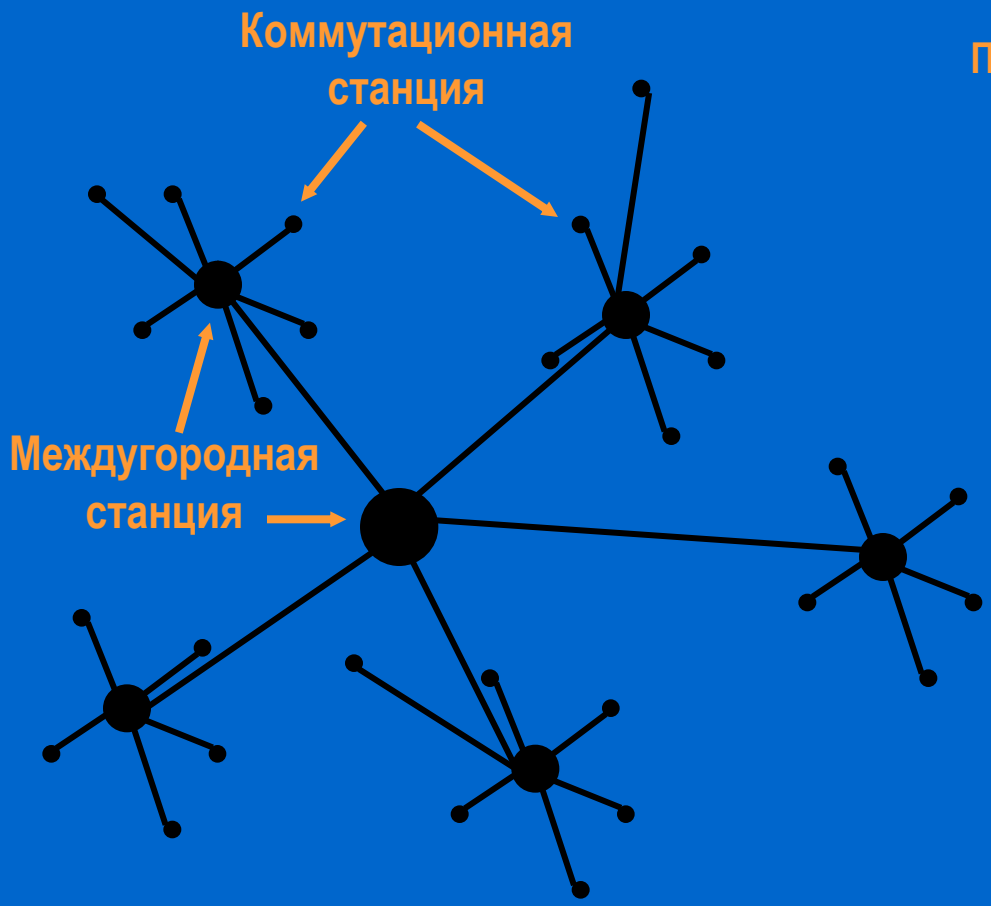
Реальная передача битов по каналу связи. Кабели, разъемы, электрические параметры сигналов.

Эталонные модели

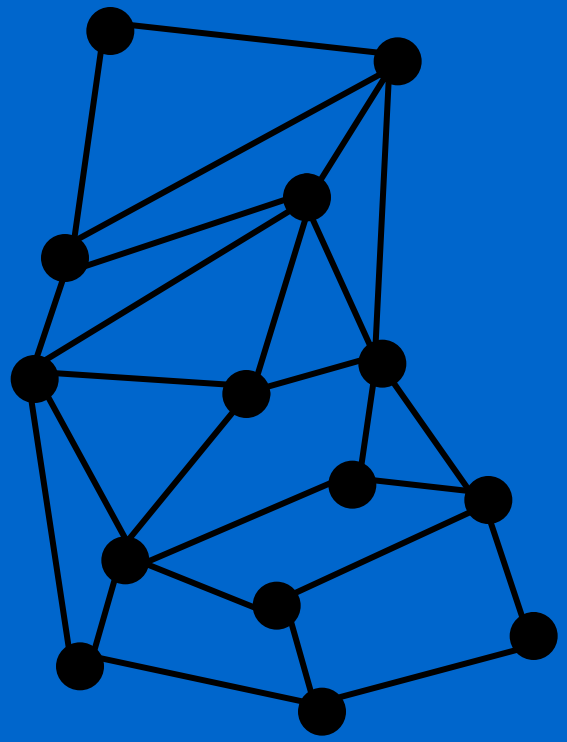
Эталонная модель TCP / IP

Бабушка ARPANET

Пол Бэрен (RAND) 1957 год – AT & T отвергла



Структура телефонной сети



Архитектура распределенной сети

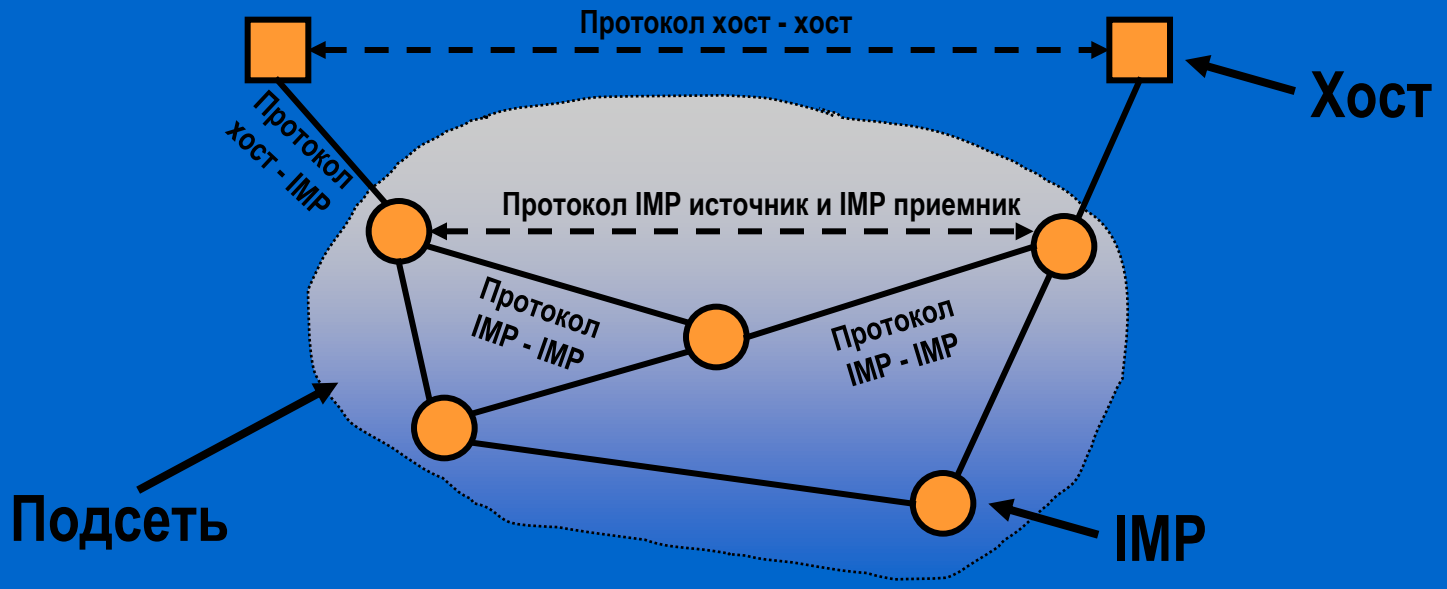
Эталонные модели

Эталонная модель TCP / IP (ARPANET)

ARPA – Advanced Research Project Agency (Управление перспективного планирования научно-исследовательских работ)

(1957 год) 1967 год – Англия, Дональд Дэвис

Подсеть из IMP (Interface Massage Processor), линии связи, пакеты, 56 Кбит/сек, каждый IMP связан с двумя, дейтаграммы. Хост – IMP: сообщения до 8063 бит – пакеты по 1008 бит.

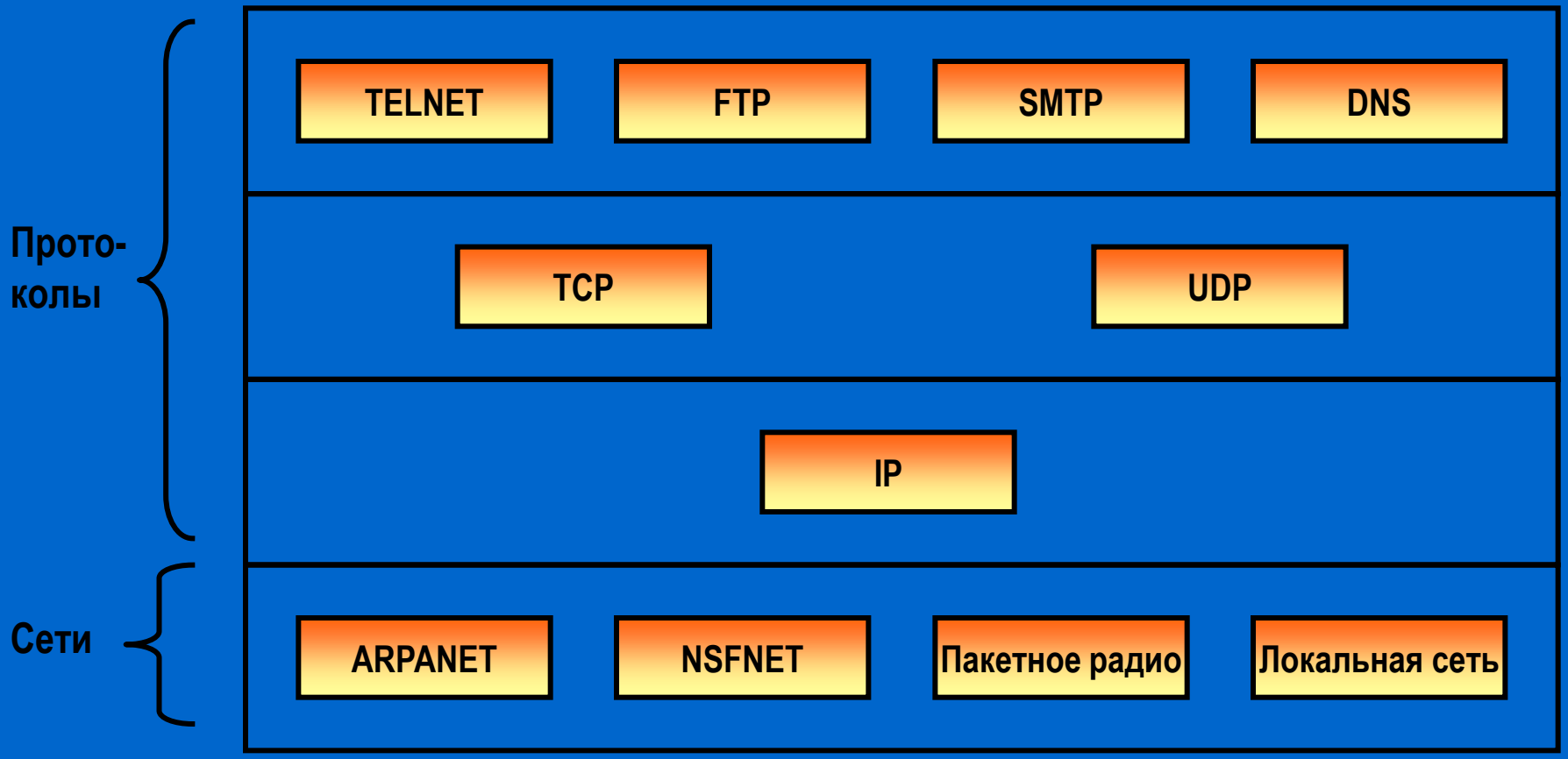


Декабрь 1969 – 4 узла (Лос-Анжелес, Санта Барбара, Стэнфорд и Юта). Сентябрь 1972 более 30.

TCP/IP (ЛС к ARPANET). 80-е годы DNS (Domain Name System).

Эталонные модели

Эталонная модель TCP / IP (ARPANET)

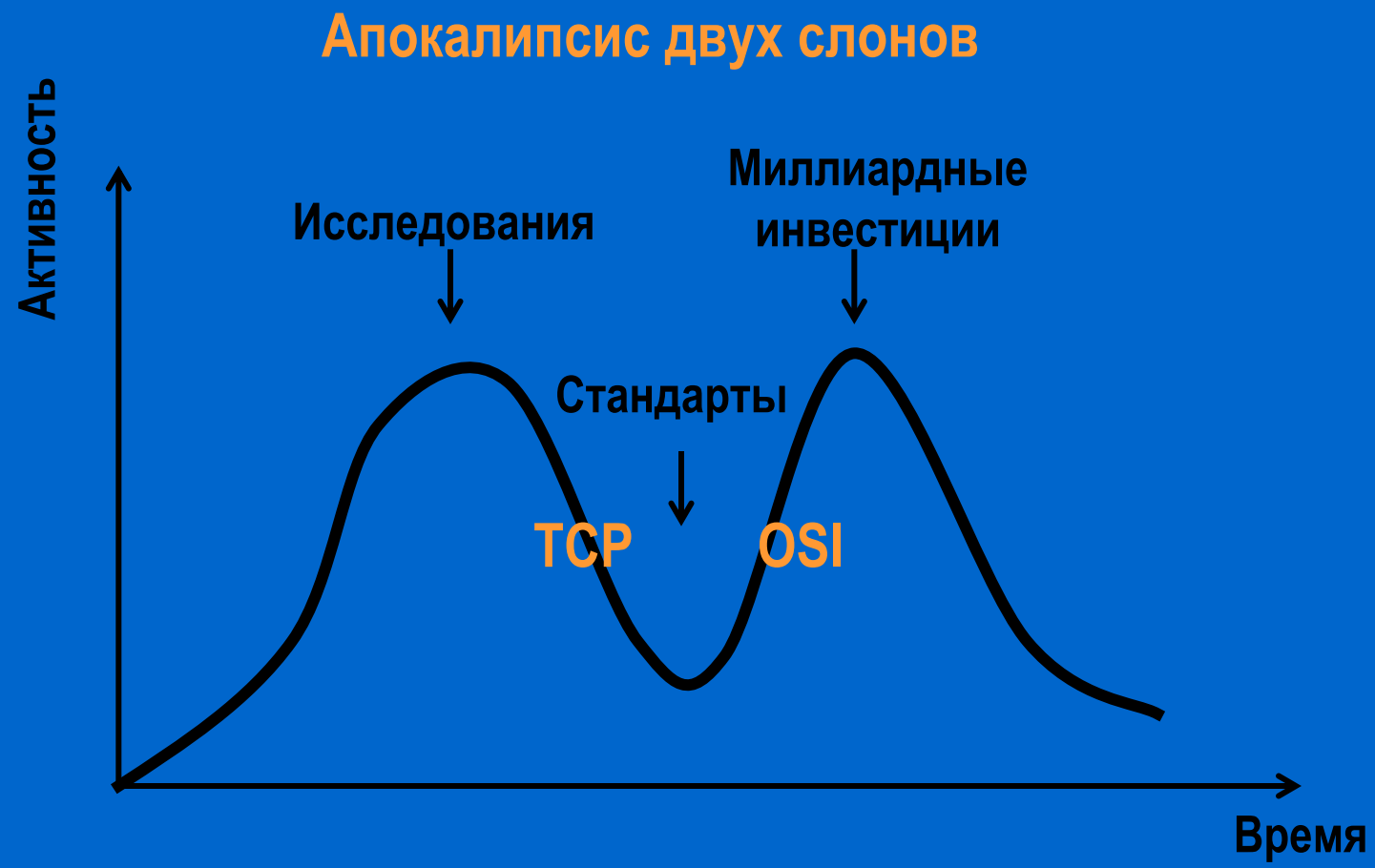


Эталонные модели OSI и TCP

Уровни протоколов и соответствия

Эталонные модели OSI и TCP

Теория стандартов Дэвида Кларка



Гибридная модель

5 уровней протоколов

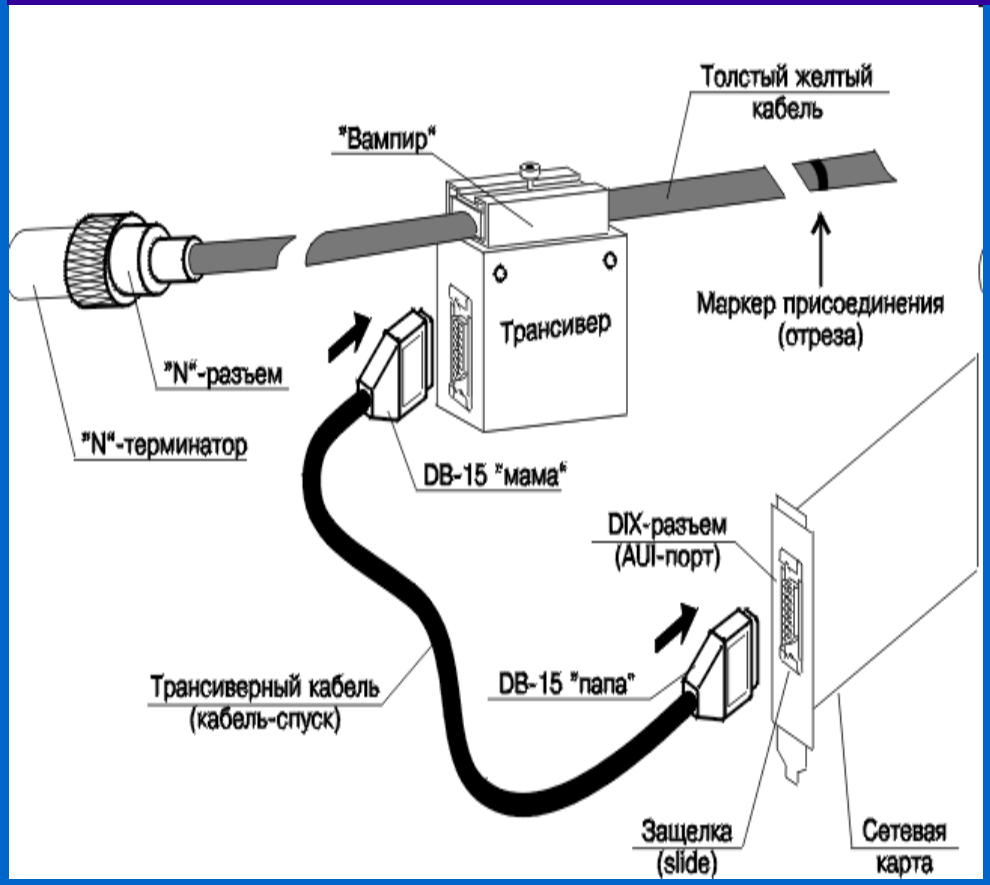
Среды передачи информации

Кабельные и бескабельные каналы

- **коаксиальные кабели** (coaxial cable);
- **кабели на основе витых пар** (twisted pair); экранированные (shielded twisted pair, STP); неэкранированные (unshielded twisted pair, UTP);
- **оптоволоконные кабели** (fiber optic);
- **бескабельные каналы** передачи информации.

Среды передачи информации

«Толстый» Ethernet (10Base5)



Скорость работы 10 Мбит/сек

Максимальная длина сегмента **500 м**

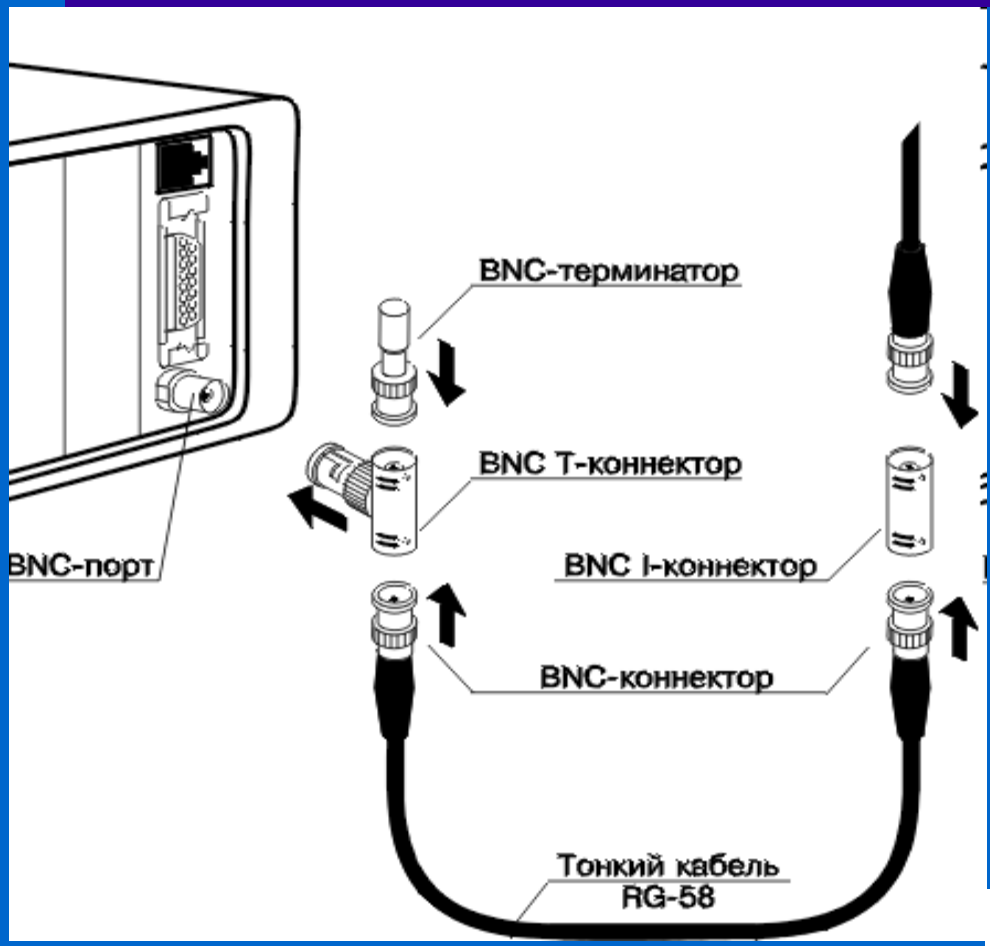
Максимальное количество компьютеров **100 / сегмент**

Максимальная общая длина сети **2500 м**

Особенности: устарел

Среды передачи информации

«Тонкий» Ethernet (10Base2)



Скорость работы 10 Мбит/сек

Максимальная длина сегмента **185 м**

Соединение с сетевой картой
BNC T-коннектор

Максимальное количество компьютеров
30 / сегмент

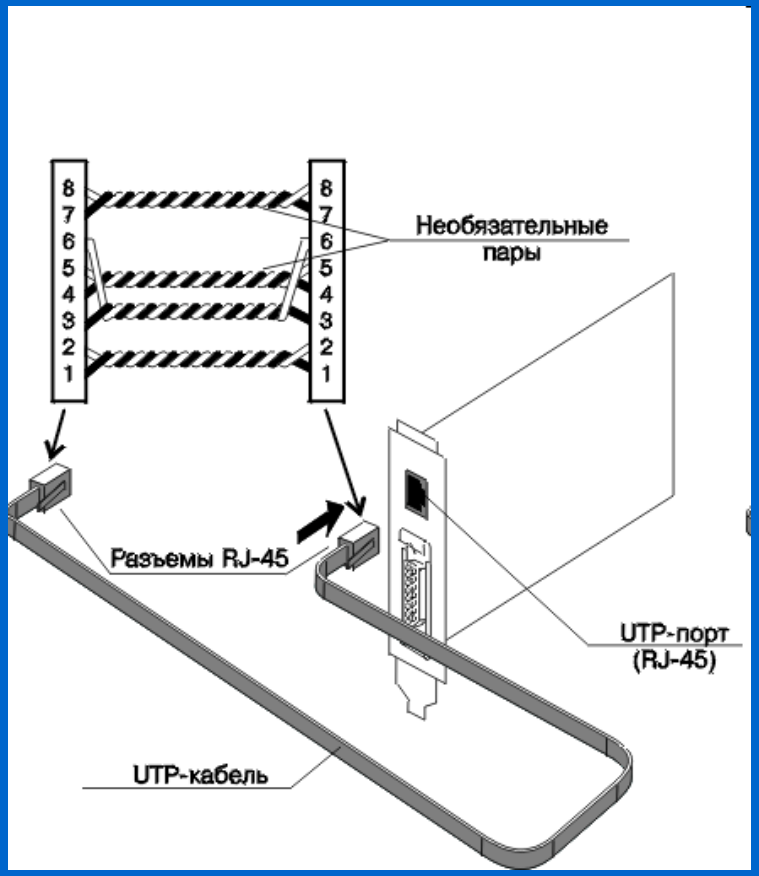
Максимальная общая длина сети **925 м**

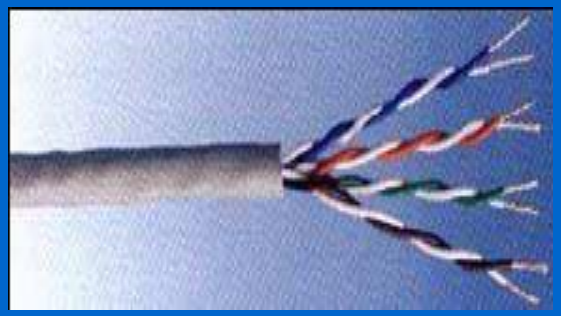
Общее число компьютеров до 1024

Особенности: не нужны концентраторы

Среды передачи информации

Ethernet на витой паре (10Base-T)





Скорость работы 10 Мбит/сек

Максимальная длина сегмента **100 м**

Соединение с сетевой картой **RJ-коннектор**

Общее число компьютеров до 1024

Особенности: низкая цена

Среды передачи информации

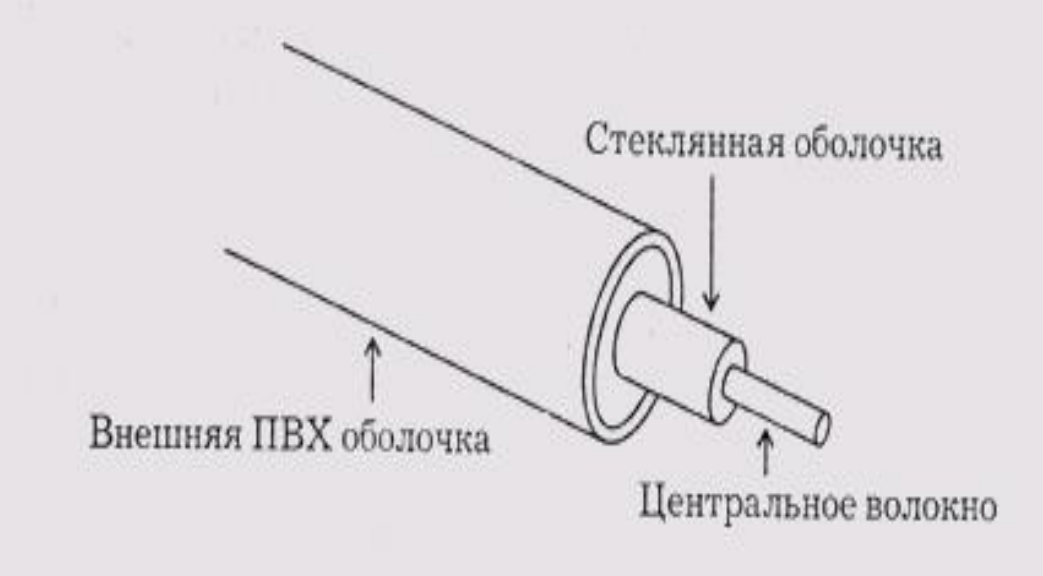
Категории витых пар (UTP- unshielded twisted pair)

- **1 категория** – обычный телефонный кабель
- **2 категория** – полоса частот до 1 Мгц
- **3 категория** – полоса частот до 16 мгц (9 вит/м)
- **4 категория** – полоса частот до 20 Мгц
- **5 категория** – полоса частот до 100 Мгц (27 вит/м)
  30-50% дороже 3 категории
- **6 категория** – полоса частот до 200 Мгц
- **7 категория** – полоса частот до 600 Мгц

Среды передачи информации

Ethernet на оптоволокне (10Base-F)

Электромагнитных помех нет



Скорость работы 10 Мбит/сек

Максимальная длина сегмента 2000 **м**

Максимальное количество компьютеров 1024 / сегмент

Среды передачи информации

Кабели для быстрого Ethernet

100 Мбит/сек

Название	Тип	Длина сегмента	Особенности
100Base-T4	Витая пара	100 м	Использование неэкранированной витой пары категории 3
100Base-TX	Витая пара	100 м	Полный дуплекс при 100 Мбит/сек (витая пара категории 5)
100Base-FX	Оптоволокно	2000 м	Полный дуплекс при 100 Мбит/сек; большая длина сегмента

Среды передачи информации

Кабели гигабитного Ethernet

1000 Мбит/сек (1 Гбит/сек)

Название	Тип	Длина сегмента	Особенности
1000Base-SX	Оптоволокно	550 м	Многомодовое волокно (50, 62.5 мкм)
1000Base-LX	Оптоволокно	5000 м	Одномодовое (10 мкм) волокно или многомодовое (50, 62.5 мкм) волокно
1000Base-CX	2 экранированные витые пары	25 м	Экранированная витая пара
1000Base-T	4 неэкранированные витые пары	100 м	Стандартная витая пара 5-й категории

Наименование величин

Префиксы

Степень	Префикс	Степень	Префикс
-3	Милли	3	Кило
-6	Микро	6	Мега
-9	Нано	9	Гига
-12	Пико	12	Тера
-15	Фемто	15	Пета
-18	Атто	18	Экза
-21	Цепто	21	Цетта
-24	Йокто	24	Йота

Среды передачи информации

Бескабельные каналы

- **Радиоканалы**
  - одночастотные
  - в рассеянном спектре
  - сотовые
- **Инфракрасные каналы**
  - прямой видимости
  - на рассеянном излучении

Среды передачи информации

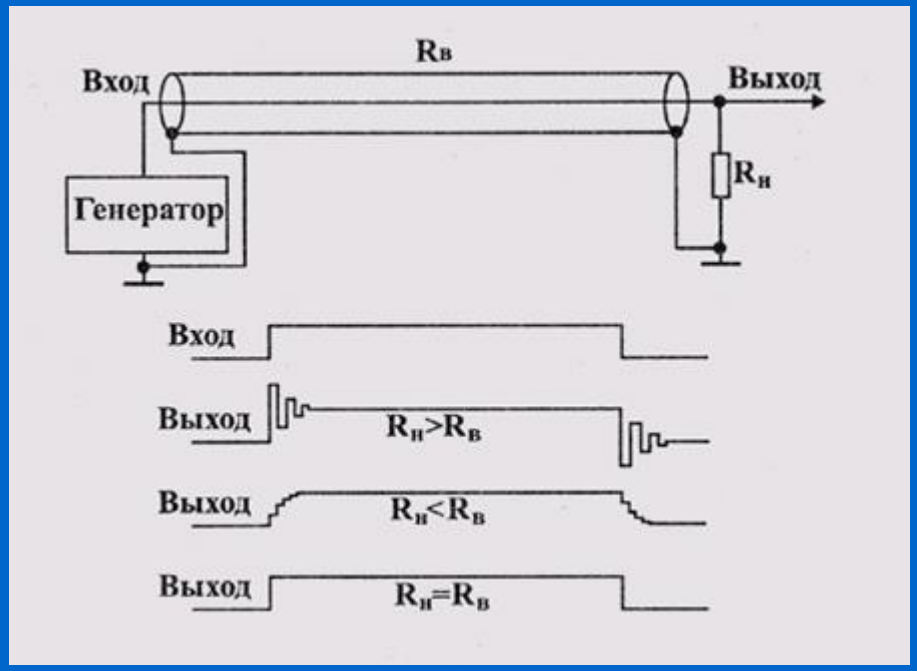
Факторы влияющие на качество передачи

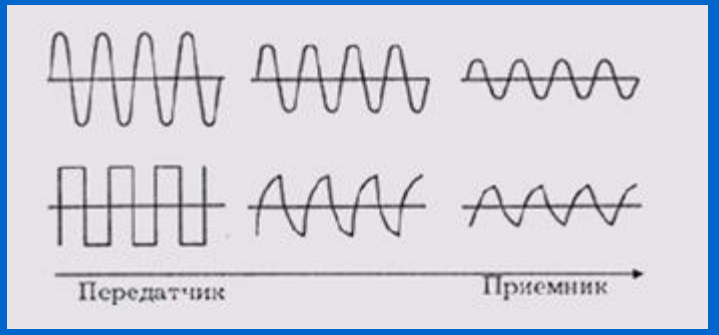
- **Согласование** электрических линий
- **Экранирование** электрических линий
- **Гальваническая развязка** компьютеров

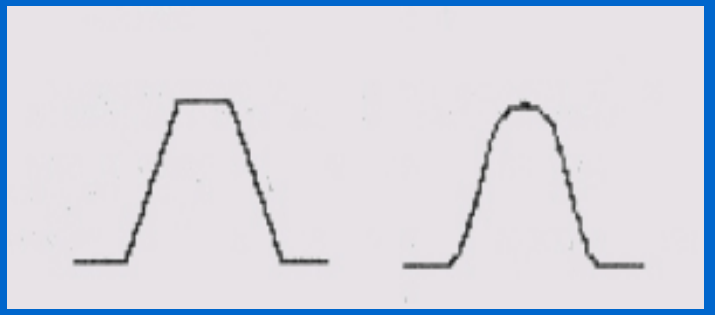
Среды передачи информации

Согласование линий связи

Применяется для обеспечения нормального прохождения сигнала по длинной линии без отражений и искажений



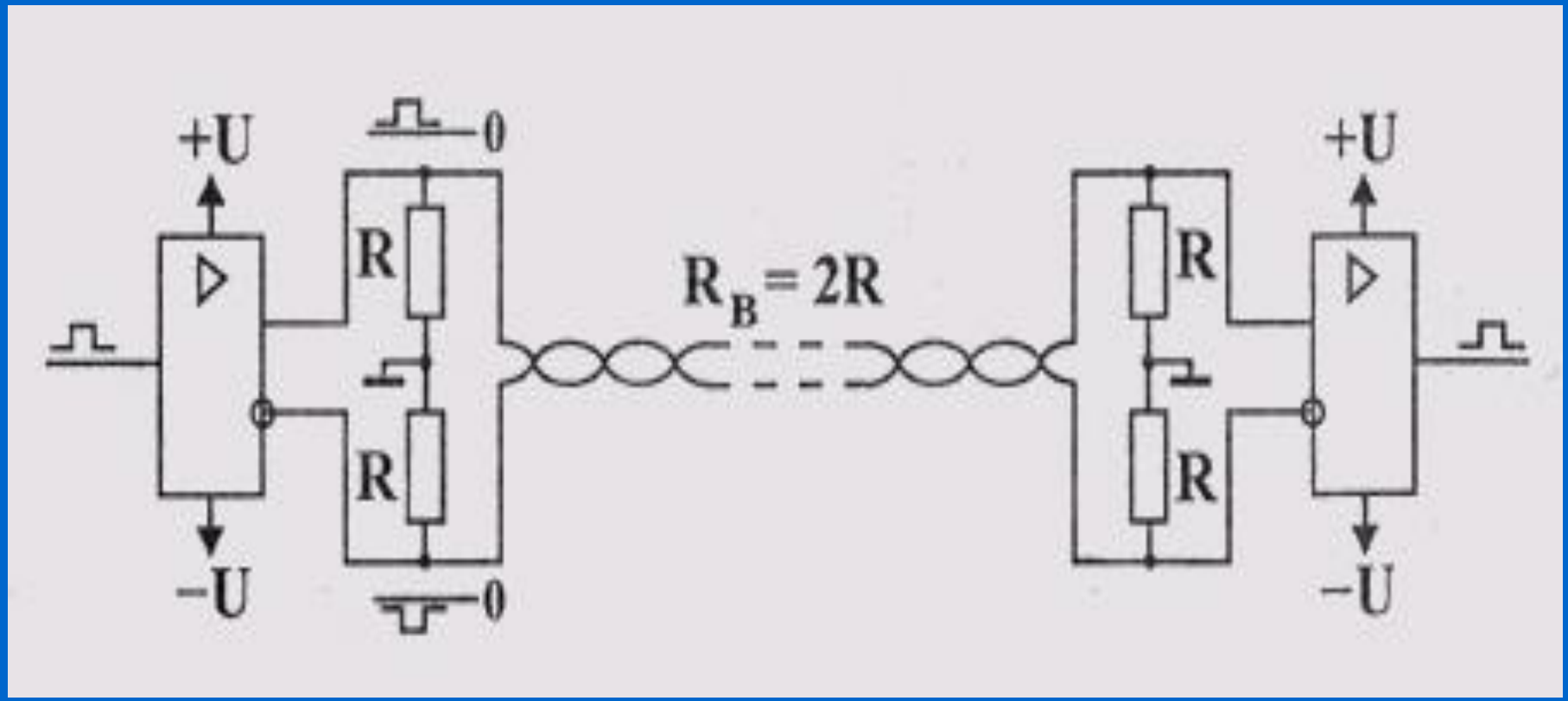




Среды передачи информации

Экранирование линий связи

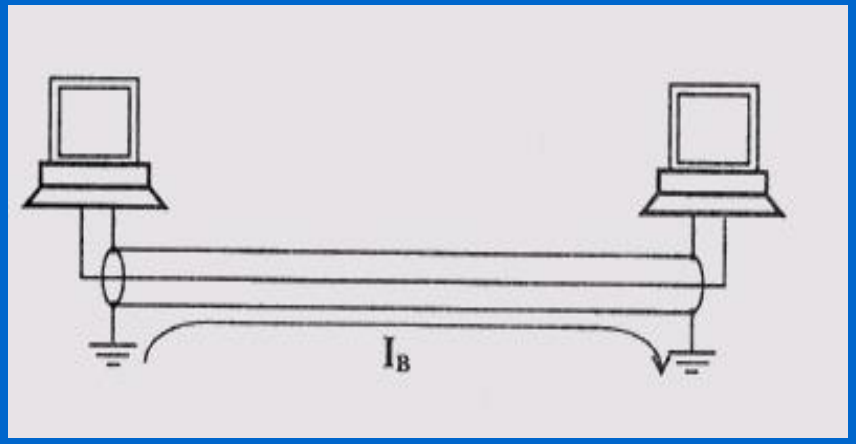
Дифференциальная передача сигналов снижает влияние наведенных помех

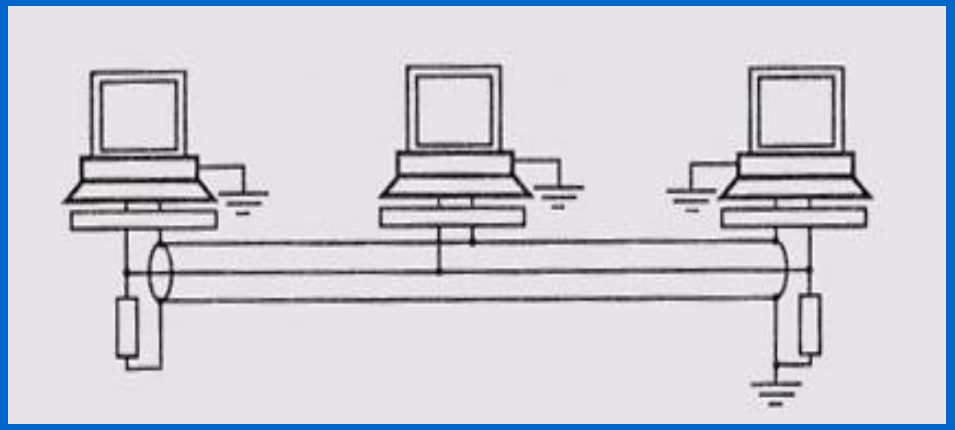


Среды передачи информации

Гальваническая развязка

Трансформаторная гальваническая развязка входит в состав каждого сетевого адаптера

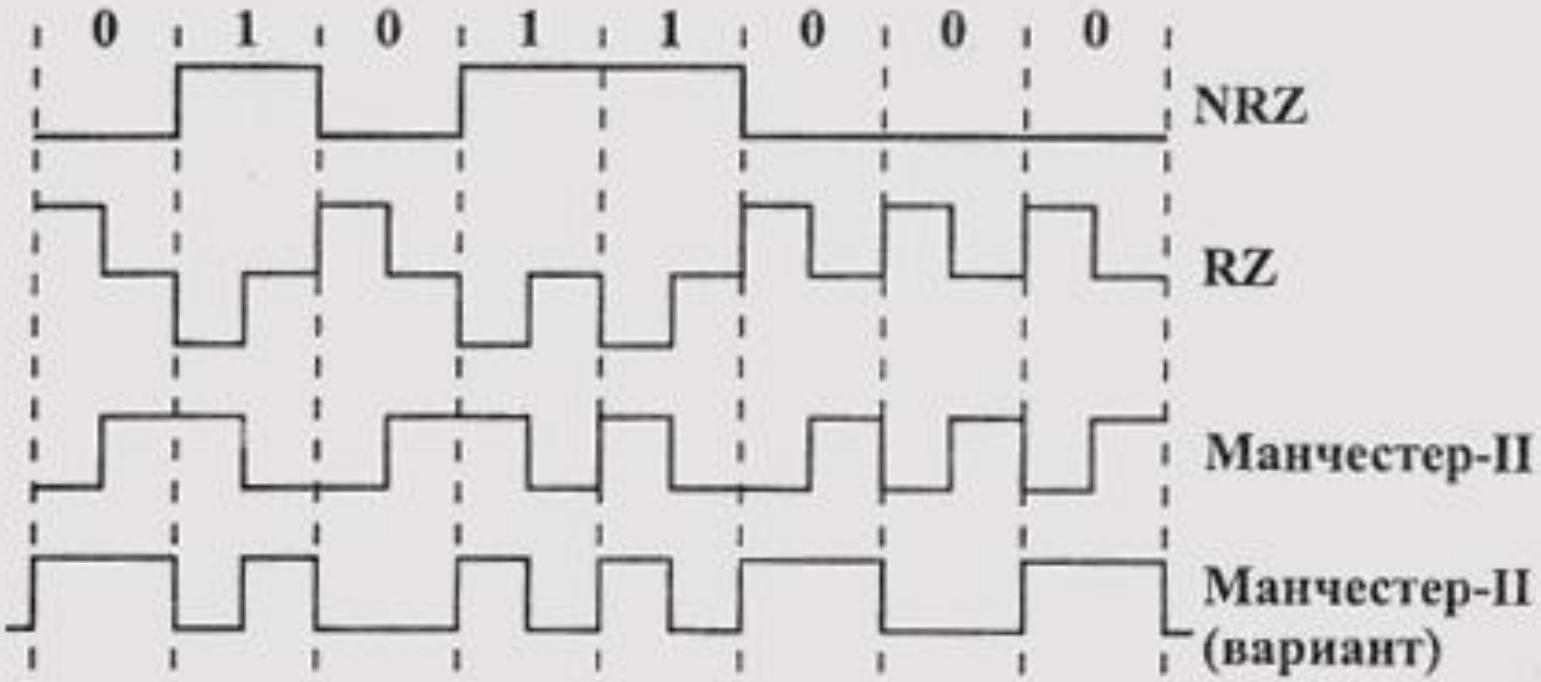




Кодирование информации в ЛС

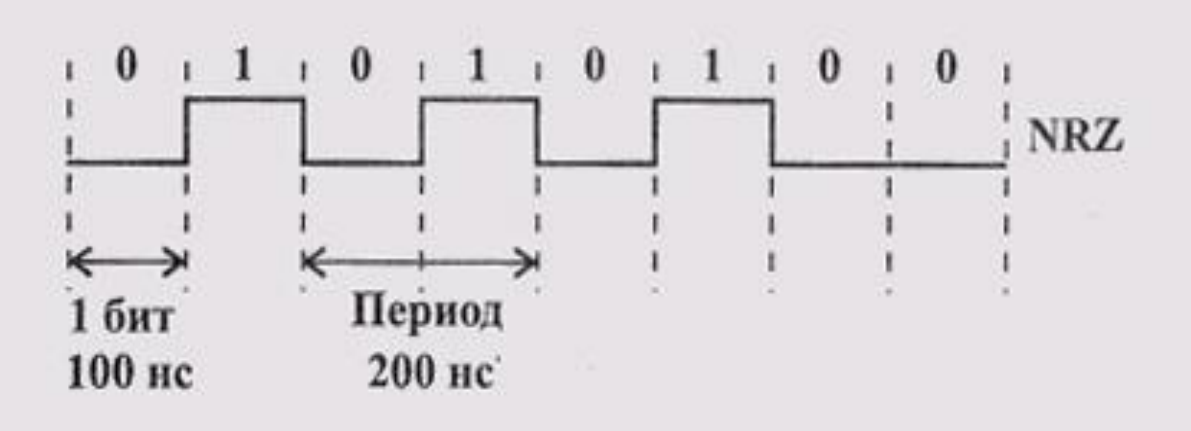
Коды передачи информации

- Non Return to Zero (NRZ)
- Return to Zero (RZ)

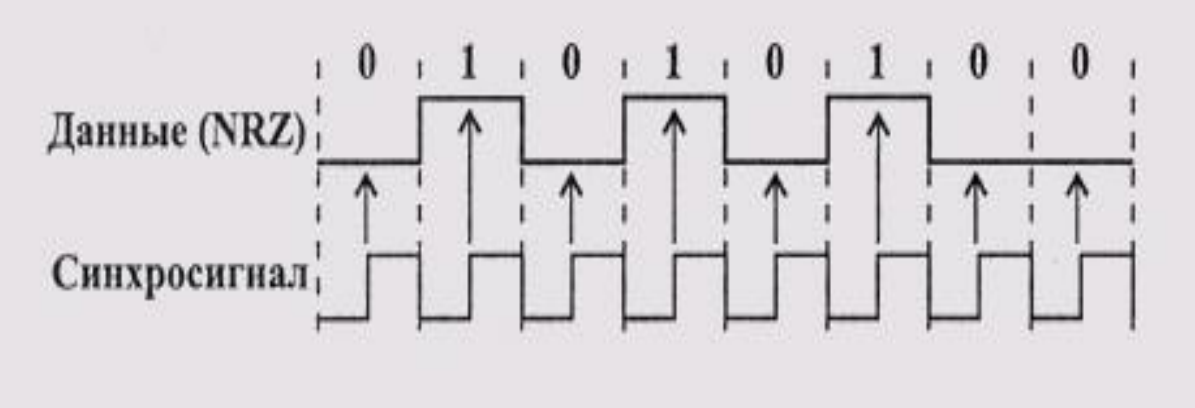


Кодирование информации в ЛС

Требуемая пропускная способность линии

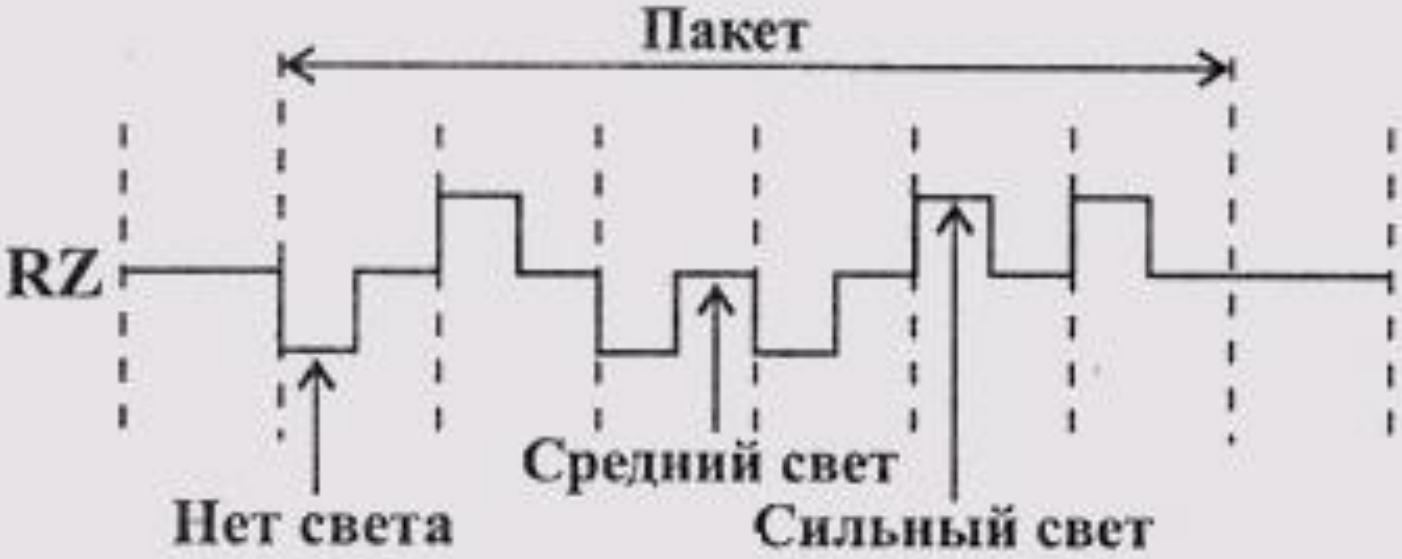


- скорость передачи 10 Мбит/сек
- требуемая пропускная способность линии составит 1 / 200нс = 5 МГц



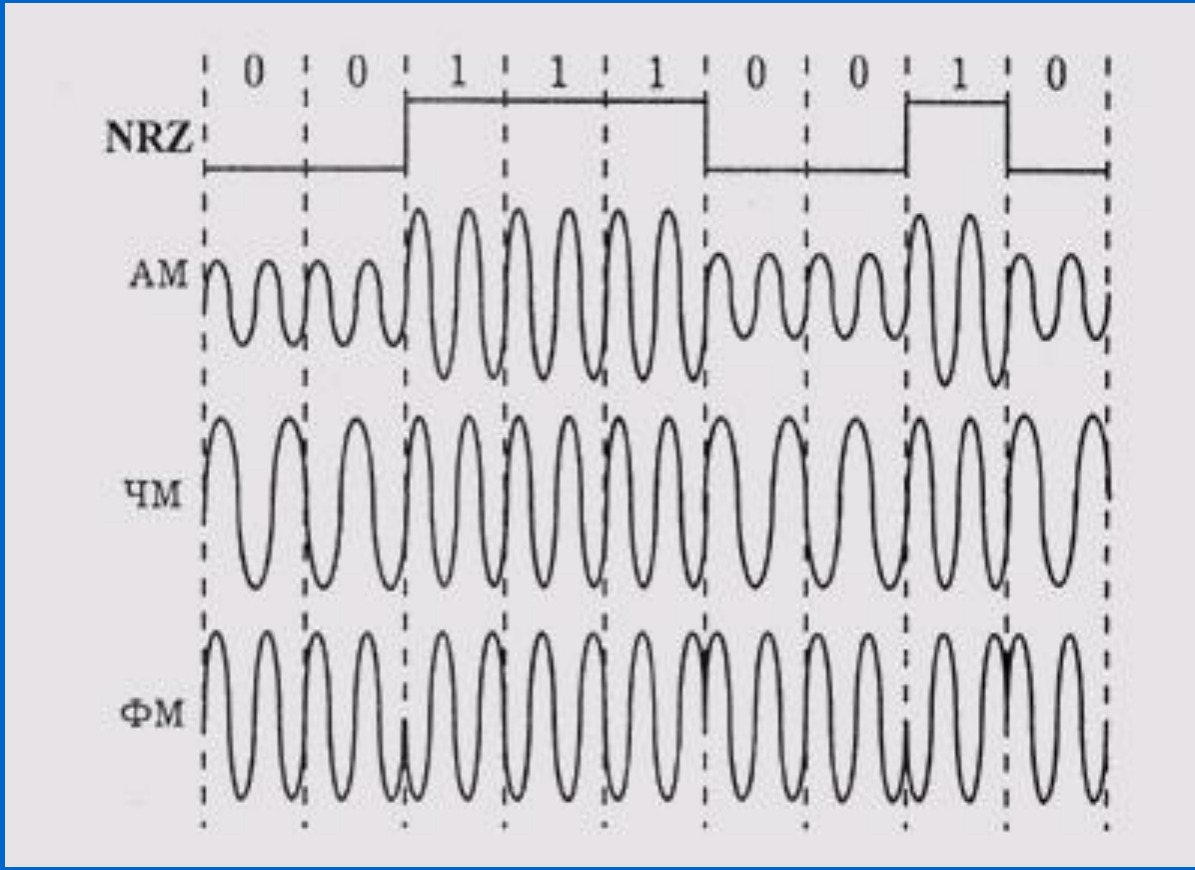
Кодирование информации в ЛС

RZ код в оптоволоконных сетях



Кодирование информации в ЛС

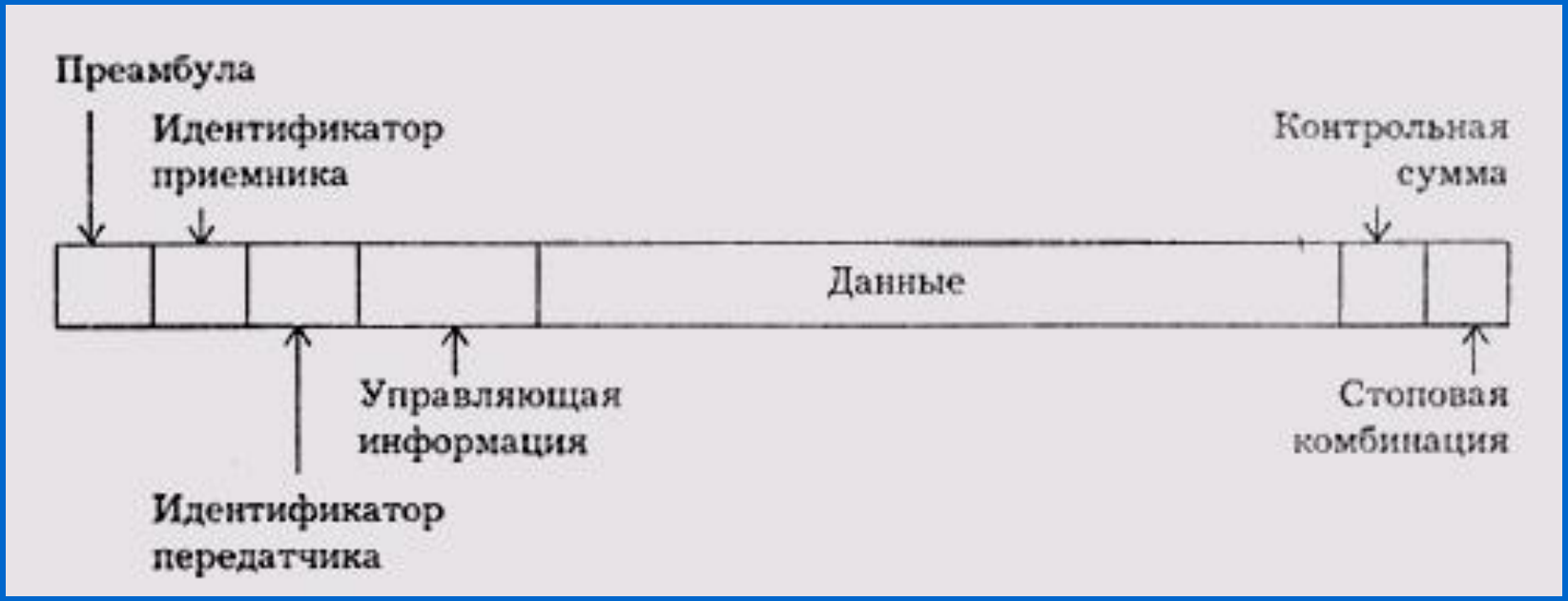
Аналоговое кодирование цифровой информации



Кадры, пакеты

Типичная структура пакета

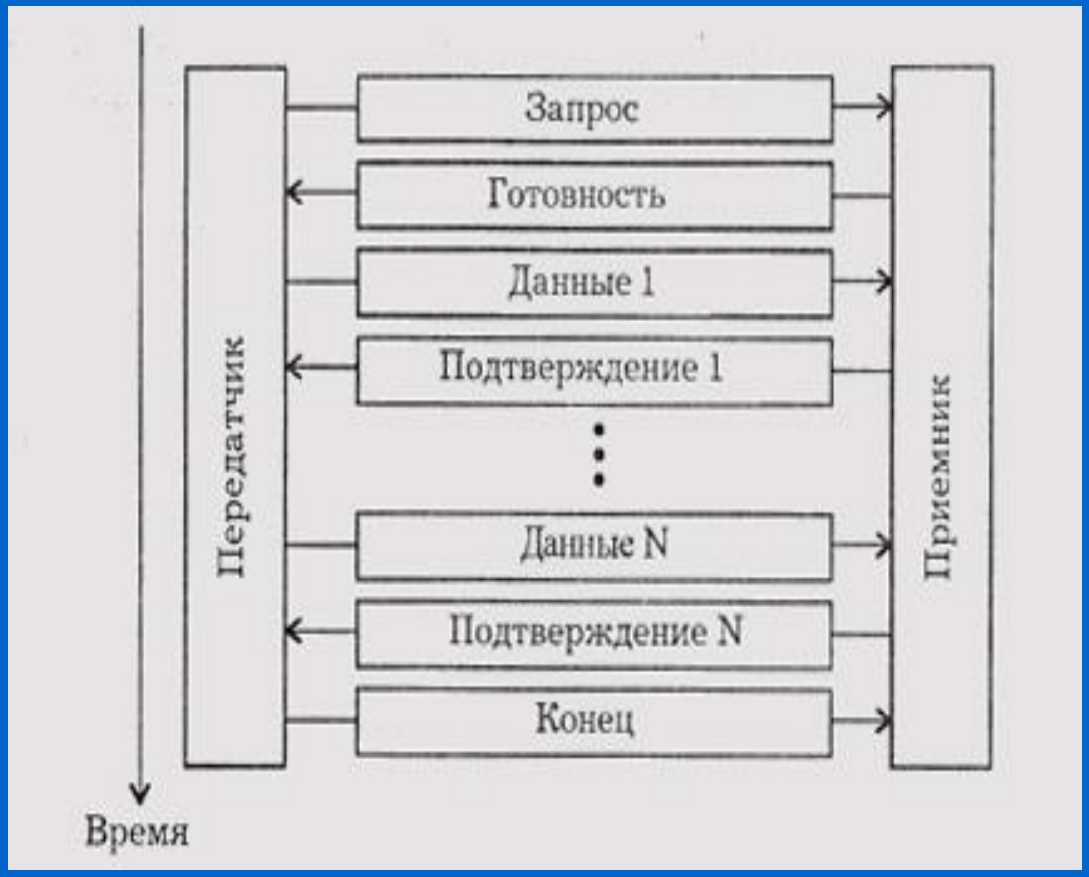
Заголовок **Трейлер**



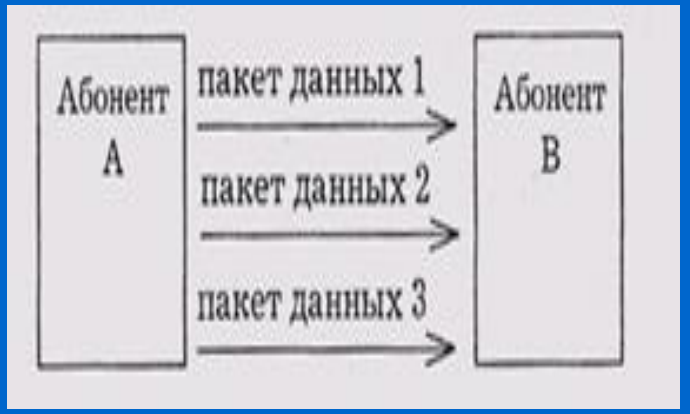
Кадры, пакеты

Обмен пакетами при сеансе связи

Обмен с логическим соединением
(с подтверждением, с гарантированной доставкой)

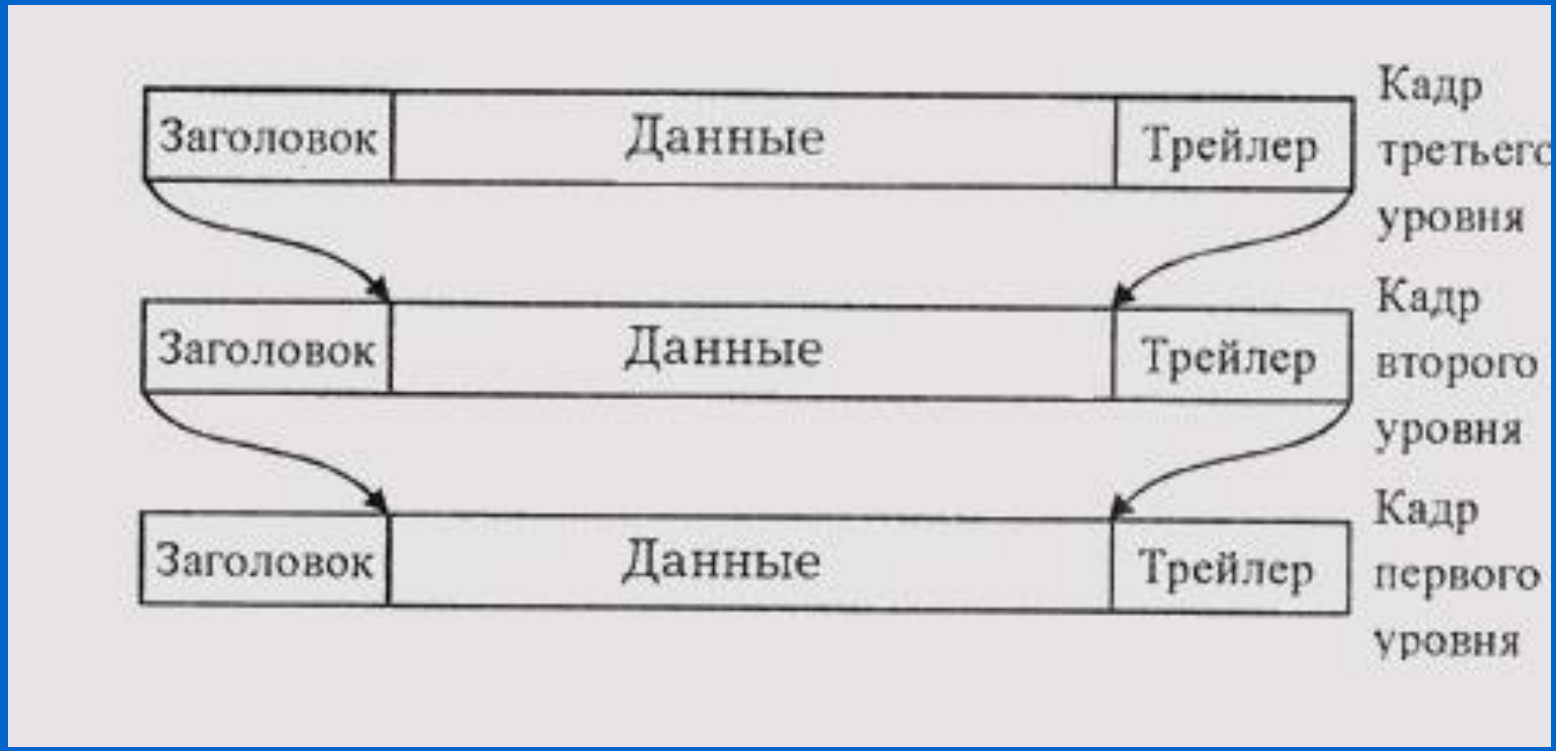


Метод дейтаграмм



Кадры, пакеты

Многоуровневое вложение кадров

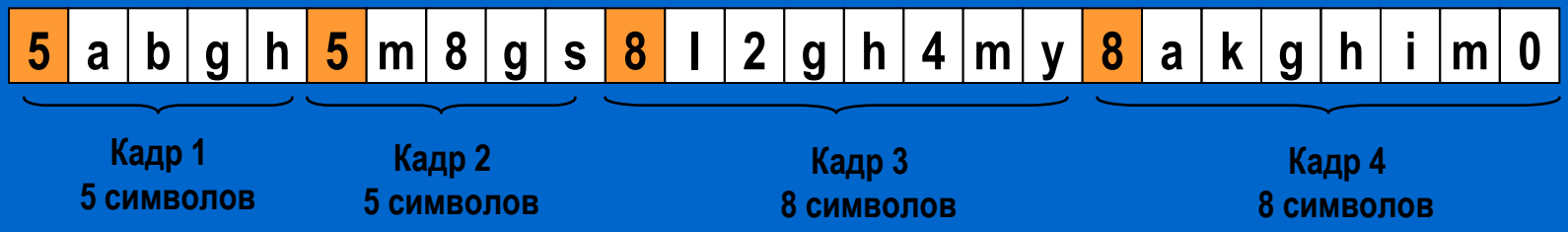


При обмене по сети используются многоуровневые протоколы, каждый из которых предполагает свою структуру кадра (свою адресацию, свою управляющую информацию, свой формат данных)

Формирование кадра

Методы маркировки границ

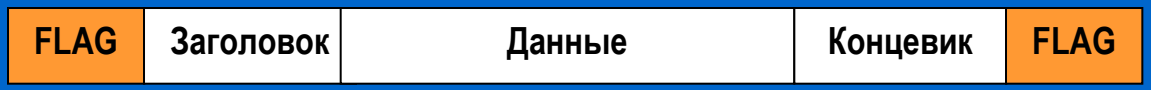
1. Подсчет количества символов
2. Использование сигнальных байтов с символьным заполнением
3. Использование стартовых и стоповых битов с битовым заполнением
4. Использование запрещенных сигналов физического уровня

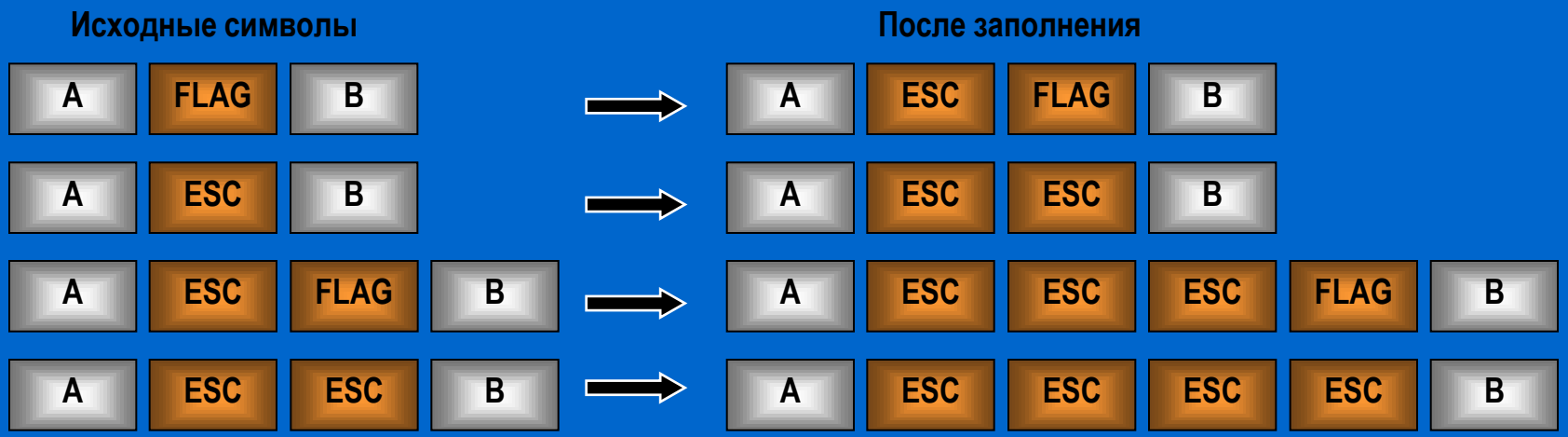


Формирование кадра

Методы маркировки границ

1. Подсчет количества символов
2. Использование сигнальных байтов с символьным заполнением
3. Использование стартовых и стоповых битов с битовым заполнением
4. Использование запрещенных сигналов физического уровня





Формирование кадра

Методы маркировки границ

1. Подсчет количества символов
2. Использование сигнальных байтов с символьным заполнением
3. Использование стартовых и стоповых битов с битовым заполнением
4. Использование запрещенных сигналов физического уровня

01111110

Стартовая и стоповая последовательность битов

011011111111111111110010

Исходные данные

011011111011111011111010010

Данные на линии передачи (0 -вставленные биты)

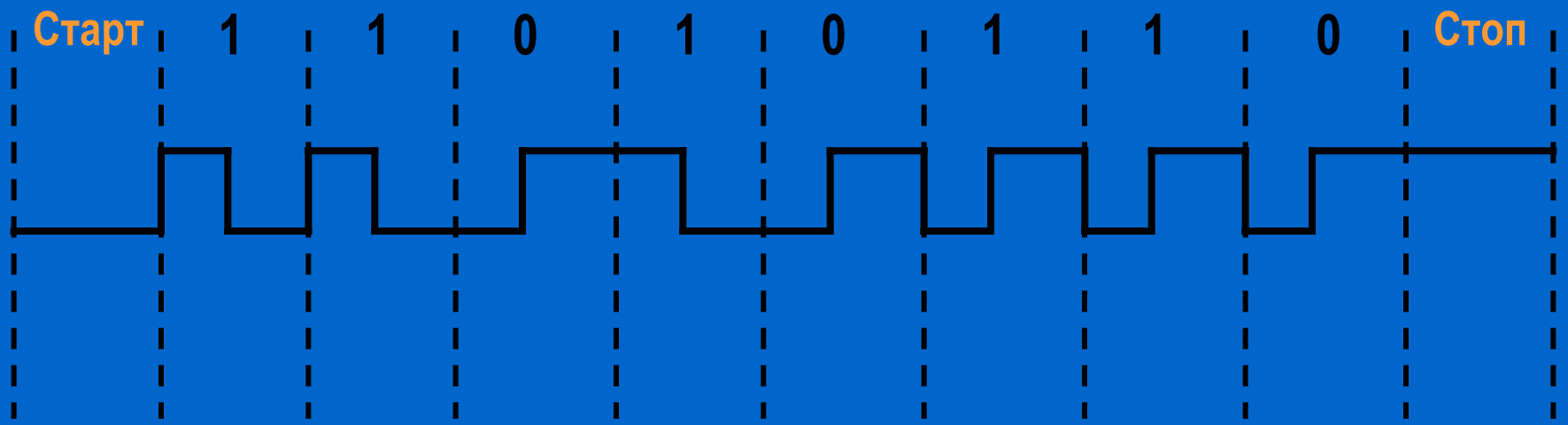
011011111111111111110010

Принятые данные после обработки

Формирование кадра

Методы маркировки границ

1. Подсчет количества символов
2. Использование сигнальных байтов с символьным заполнением
3. Использование стартовых и стоповых битов с битовым заполнением
4. Использование запрещенных сигналов физического уровня



Формирование кадра

Корректирующее кодирование

1. **Коды с исправлением ошибок – беспроводные каналы**
2. **Коды с обнаружением ошибок – оптоволоконные каналы**

Полная длина кадра $n = m + r$, m – информационные биты

r – контрольные (избыточные) биты

Кодовое расстояние по Хэммингу

$$\begin{array}{r} 10001001 \\ \oplus\ 10110001 \\ \hline 00111000 \end{array} \qquad d = 3$$

2^m - допустимы все

2^n - допустимы не все

d_{min} - минимальное кодовое расстояние

Для обнаружения d ошибок необходим код с $d_{min} = d + 1$

Для исправления d ошибок необходим код с $d_{min} = 2d + 1$

Формирование кадра

Корректирующее кодирование

1. Коды с исправлением ошибок – беспроводные каналы
2. Коды с обнаружением ошибок – оптоволоконные каналы

0000000000 0000011111 1111100000 1111111111

$d_{min} = 5$ 0000000111 0000011111

Создадим код $m + r$ способный исправлять все одиночные ошибки. Каждому из 2^m допустимых сообщений должны соответствовать $n + 1$ кодовых комбинаций

$$2^n \Rightarrow (n + 1)\, 2^m \leq 2^n$$

$$n = m + r \Rightarrow \boxed{m + r + 1 \leq 2^r}$$

Формирование кадра

Корректирующий код Хэмминга

Символ	ASCII	Контрольные биты 1 2 4 8
H	1001000	00110010000
a	1100001	10111001001
m	1101101	11101010101
m	1101101	11101010101
i	1101001	01101011001
n	1101110	01101010110
g	1100111	01111001111
	0100000	10011000000
c	1100011	11111000011
o	1101111	10101011111
d	1100100	11111001100
e	1100101	00111000101

Бит данных k-ой позиции входит в несколько контрольных сумм:
k = 11 (8,2,1) k = 29 (16,8,4,1)

Когда прибывает кодовое слово, приемник обнуляет счетчик. Затем проверяется каждый контрольный бит k (k =1,2,4,8,…) на четность. Если сумма нечетная, к счетчику добавляется число k. Если после всех проверок счетчик равен 0, нет ошибок. В противном случае - в счетчике номер неверного бита.

Формирование кадра

Корректирующее кодирование

1. Коды с исправлением ошибок – беспроводные каналы
2. Коды с обнаружением ошибок – оптоволоконные каналы

1000 бит r = 10 Матрица n x k

1 Мегабит r = 10000 Вероятность необнаружения 2^{-n}

CRC – Cyclic Redundancy Check – Циклический избыточный код

110001 – $x^5 + x^4 + x^0$

$G(x)$ – образующий многочлен (*32,26,23,22,16,12,11,10,8,7,5,4,2,1,0*)

$M(x)$ – передаваемое сообщение

$T(x) = x^r M(x) - x^r M(x) \% G(x)$ – передаваемый кадр

$[T(x) + E(x)] \% G(x) = E(x) \% G(x)$ Вероятность необнаружения 2^{-r}

Кадры

Методы управления обменом

- Централизованные методы
- Децентрализованные методы
  - детерминированные методы
  - случайные методы

Кадры

Централизованный метод управления обменом

Максимальная величина времени доступа для любого абонента будет равна суммарному времени передачи пакетов всех абонентов сети, кроме данного (здесь - четыре длительности пакета).

Кадры

Случайные методы управления обменом

В основе всех разработок лежит 5 допущений:

- Станционная модель
- Предположение о едином канале
- Допущение о коллизиях
- a) Непрерывное время b) Дискретное время
- a) Контроль несущей b) Отсутствие контроля

70-е годы ALOHA (Норман Абрамсон)

a) Чистая ALOHA b) Дискретная ALOHA (интервал = время кадра)

1-настойчивый CSMA - Carrier Sense Multiple Access

ненастойчивый CSMA

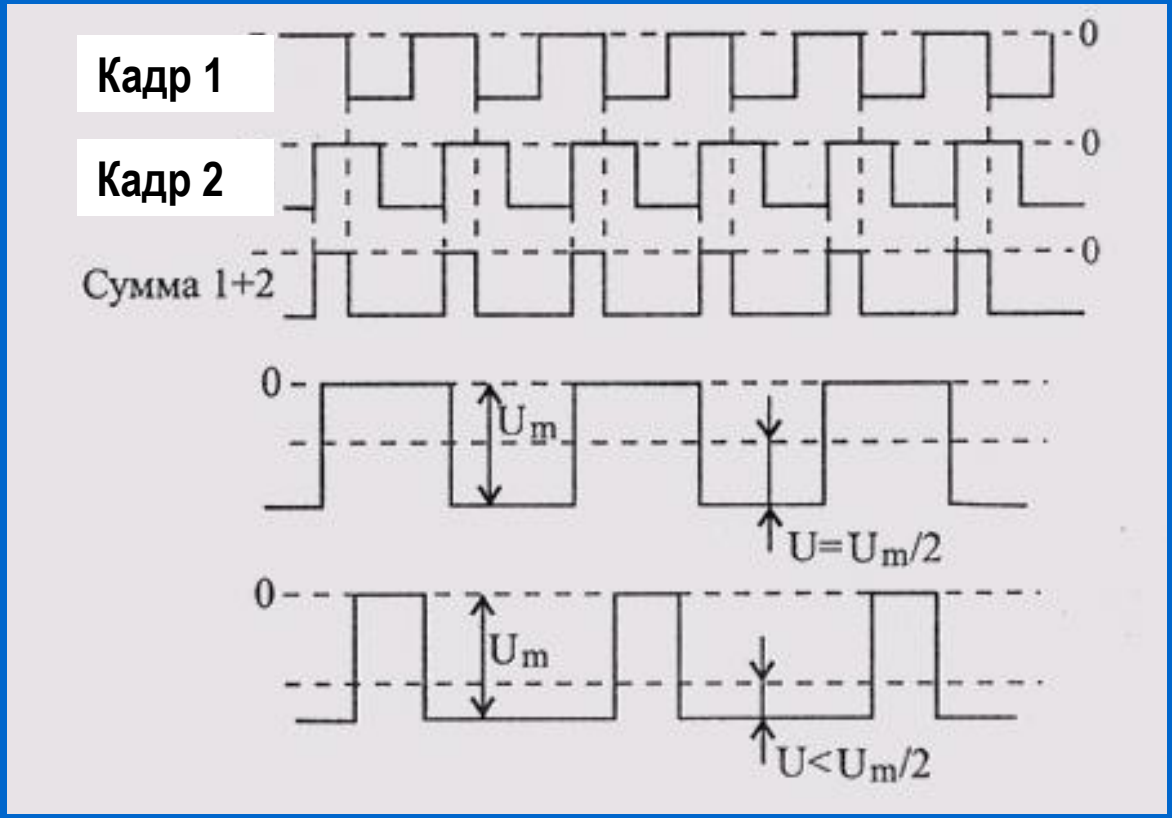
p-настойчивый CSMA

CSMA/CD - with Collision Detection (3 состояния – конкуренция, передача, простой)

Кадры

Случайные методы управления обменом

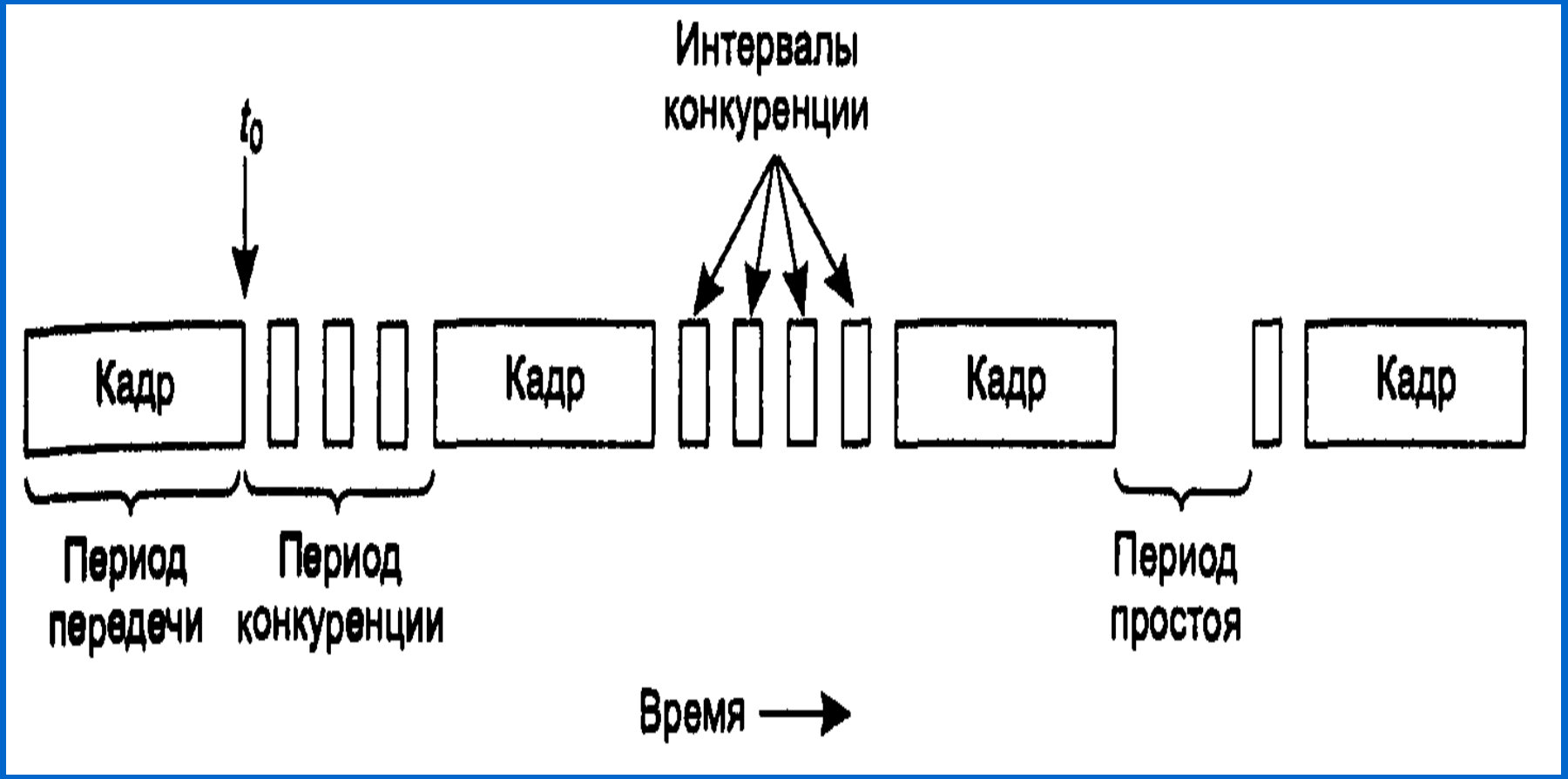
Как сетевые адаптеры распознают коллизию



Постоянная составляющая суммарного сигнала в сети будет обязательно больше или меньше половины размаха.

Кадры

Протокол CSMA/CD

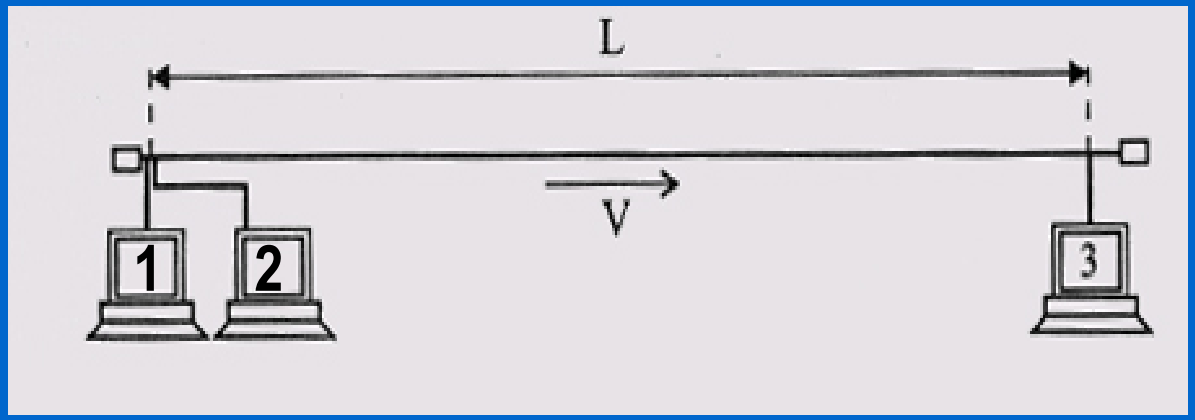


3 состояния – конкуренция, передача, простой

Кадры

Случайный метод управления обменом

Стандартный метод управления обменом CSMA/CD в Ethernet. Его главное достоинство - все абоненты полностью равноправны



PDV (Path Delay Value)

PDV = 2L/V

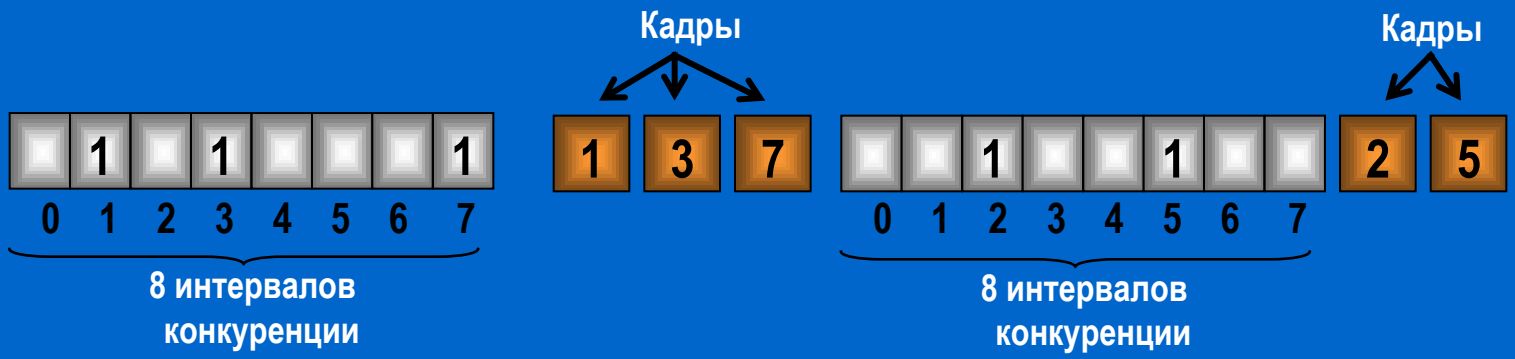
Минимально допустимая длительность кадра в сети должна составлять 2L/ V, то есть должна равняться удвоенному времени распространения сигнала по полной длине сети PDV.

Кадры

Протоколы без столкновений

1. Протокол битовой карты
2. Протокол с двоичным обратным отсчетом

Каждый период конкуренции состоит ровно из N интервалов (N рабочих станций).



Протоколы, в которых намерение передавать объявляется всем перед самой передачей, называются протоколами с резервированием.

Кадры

Протоколы без столкновений

1. Протокол битовой карты
2. Протокол с двоичным обратным отсчетом

Mok, Ward – виртуальные номера станций

C, H, D, A, G, B, E, F
7, 6, 5, 4, 3, 2, 1, 0

Станция D передала пакет

C, H, A, G, B, E, F, D
7, 6, 5, 4, 3, 2, 1, 0

Производительность в симметричном протоколе

Конфликтные и бесконфликтные протоколы. Снижение конкуренции.

Кадры

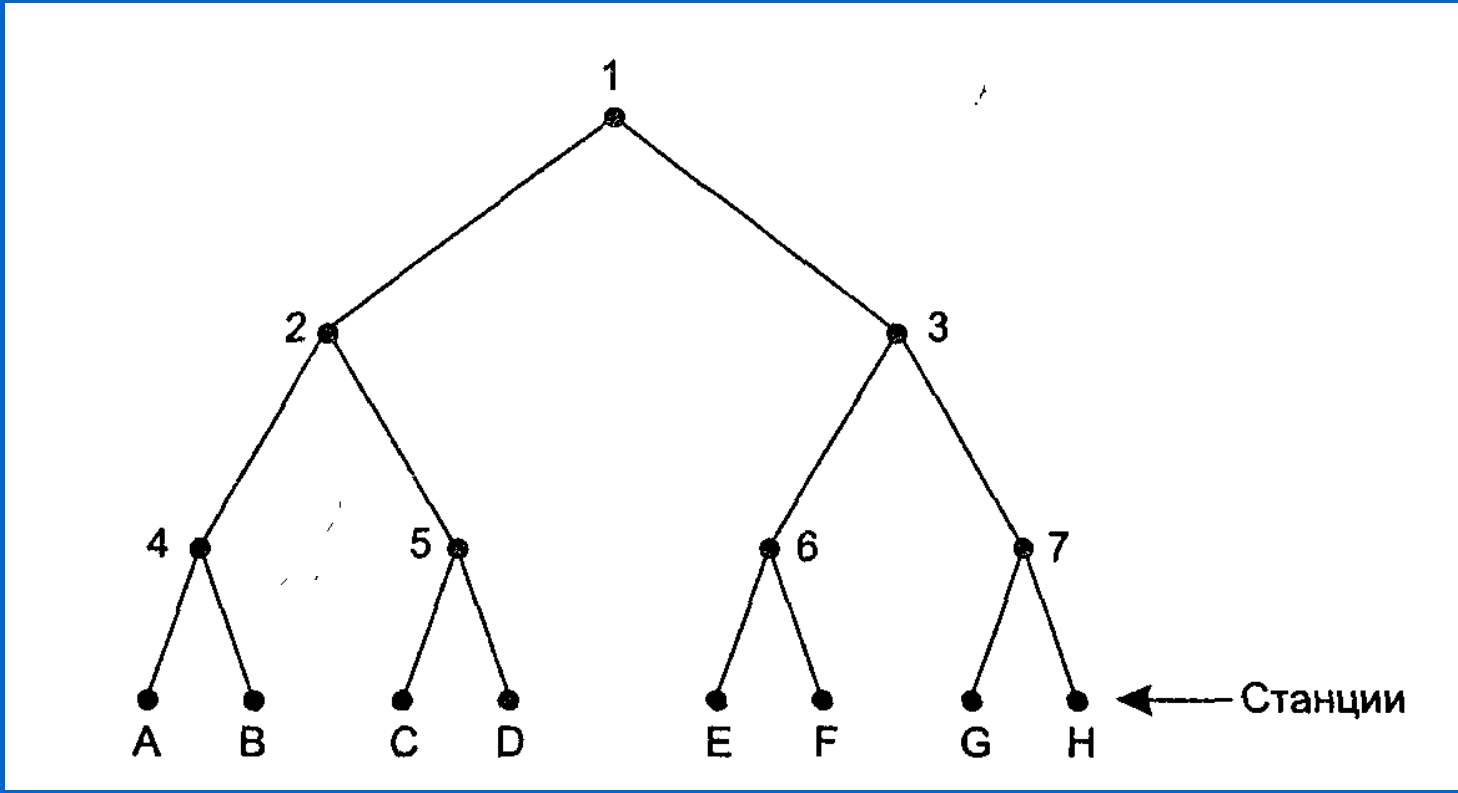
Протоколы с ограниченной конкуренцией

Уровень 0

Уровень 1

Уровень 2

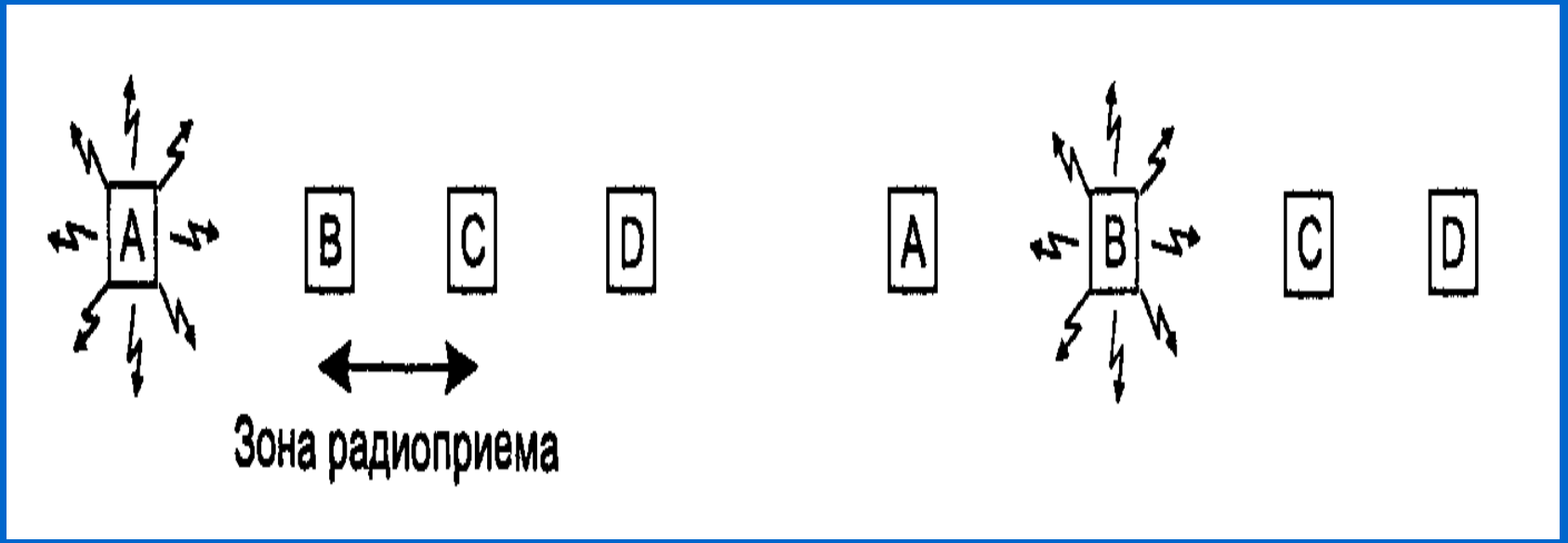
Уровень 3



Если q готовых станций распределены равномерно, то ожидаемое их число на уровне i равно $2^{-i}q$. Оптимальный уровень для начала поиска на котором $2^{-i}q = 1$. *Отсюда* $i = \log q$.

Кадры

Протоколы беспроводных сетей



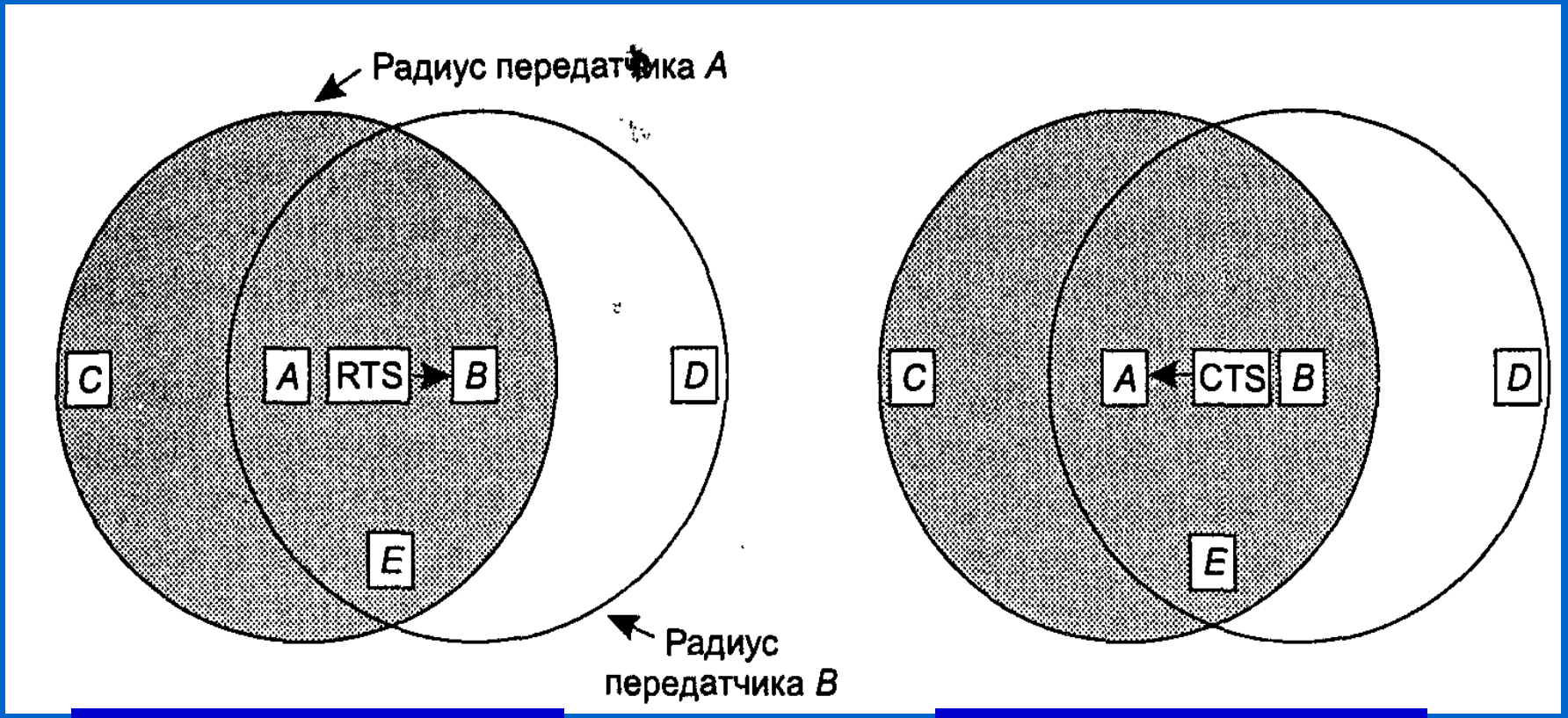
Проблема **скрытой станции**.
C передает B когда нельзя.

Проблема **засвеченной станции**.
C не передает D кода можно.

Кадры

Протоколы беспроводных сетей

MACA - Multiple Access with Collision Avoidance - множественный доступ с предотвращением столкновений – Karn, 1990



RTS – request to send

CTS – clear to send

Адресация

Физический MAC - адрес

Каждый абонент (узел) локальной сети имеет свой уникальный MAC-адрес – 48 разрядов :

- OUA (Organizationally Unique Address) – 24 разряда присваивает производитель сетевого адаптера
- OUI (Organizationally Unique Identifier) – 22 разряда IEEE присваивает каждому производителю
  OUA + OUI = UAA (Universally Administered Address) - универсально управляемый адрес или IEEE-адрес.
- I/G (Individual/Group) – 2 разряда

Адресация

Сетевой IP - адрес

Класс A – небольшое количество сетей с огромным количеством хостов 126 / 16777214
Класс B – среднее количество сетей с большим количеством хостов 16384 / 65534
Класс C – большое количество сетей с минимальным количеством хостов 2097152 / 254
Классы D и E предназначены для специального использования и не назначаются обычным сетям.

Класс	Наименьший адрес	Наибольший адрес
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Адресация

Символьный DNS - адрес

Tanya@128.11.24.41

- Тяжело запоминать
- Надо менять при переезде

Tanya@art.spb.edu

В ARPANET соответствие ASC II <–> IP-адрес в hosts.txt, но при увеличении размерности проблемы

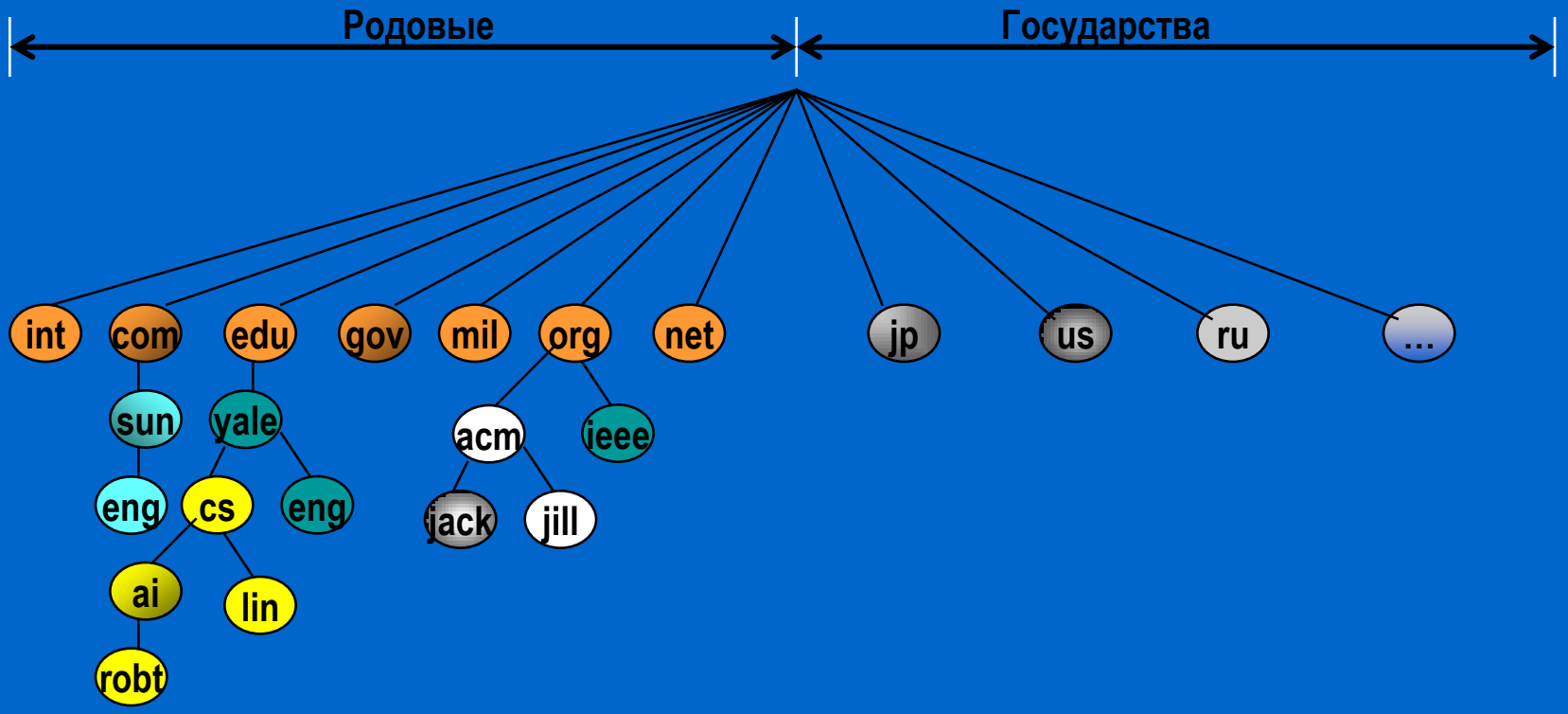
DNS – Domain Name System – служба имен доменов – иерархическая схема имен, основанная на доменах и распределенной базе данных – служит для преобразования имен хостов и пунктов назначения почты в IP-адреса

Процедура распознаватель посылает имя в виде UDP-пакета локальному DNS-серверу, который возвращает IP-адрес

Адресация

Пространство имен доменов DNS

Интернет разделен на 200 доменов верхнего уровня. Домен – множество хостов, объединенных в логическую группу. Каждый домен верхнего уровня подразделяется на поддомены. Каждый конечный домен может состоять из одного хоста или представлять компанию и состоять из тысячи хостов.



Адресация внутри локальных сетей

Протокол ARP (Address Resolution Protocol) описан в RFC 826.

При передаче пакетов внутри локальных сетей протоколы канального уровня пользуются локальными адресами узлов, отправитель же может знать только IP-адрес получателя. **Для того чтобы определить, какой локальный адрес (например, MAC-адрес в сети Ethernet) соответствует данному IP-адресу, применяется протокол ARP.** Этот протокол разрабатывался специально для Ethernet-сетей, но может работать в любых сетях, поддерживающих широковещательную передачу.

Все узлы, поддерживающие протокол ARP, ведут ARP-таблицу, состоящую из записей **<IP-адрес:MAC-адрес>**. Когда узлу нужно определить локальный адрес другого узла, его ARP- модуль сначала ищет его в ARP-таблице, и, если нужный адрес не найден, то передает широковещательное сообщение: **“Знает ли кто-нибудь локальный адрес для IP 123.45.67.89? Я 123.45.67.90, мой MAC-адрес 10:20:30:40:50:60.”. Узел, которого разыскивают, отвечает (не широковещательно, а прямой передачей): “Да, 123.45.67.89 – это я. Мой MAC-адрес 10:20:30:40:50:61”.** При этом он сохраняет пару <IP-адрес;MAC-адрес> искавшего его узла в своей ARP-таблице. Наконец, первый узел, получив ответ, заносит его в свою ARP-таблицу.

Базовые утилиты
для тестирования сетей TCP/IP

Утилита Ping позволяет проверить существование указанного узла и измерить время передачи до него одного пакета (можно задавать разные размеры пакета для исследования промежуточных сетей). Эта утилита выполняет передачу ICMP-сообщения типа 8 (Echo request), на которое получатель должен ответить ICMP-сообщением типа 0 (Echo reply).

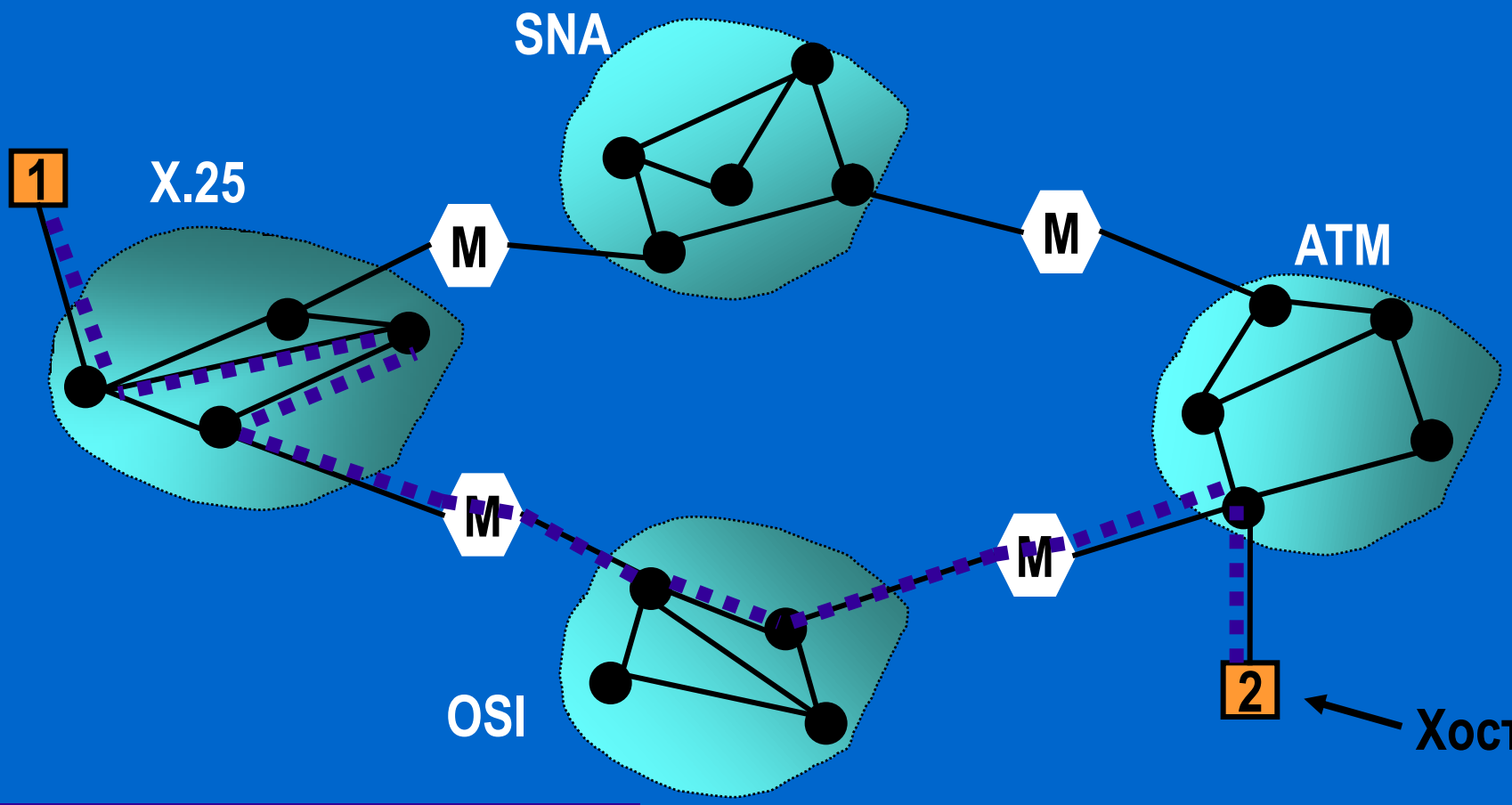
Утилита Traceroute показывает последовательность узлов, через которые проходит пакет на пути к получателю. Реализовано это следующим образом: последовательно отправляются пакеты с возрастающим значением в поле TTL: 1,2,3 и т.д. Тот маршрутизатор, который уменьшит TTL до нуля, обязан будет отправить ICMP-сообщение типа 11 (Time exceeded). В результате будут получены такие ICMP-сообщения по очереди от всех маршрутизаторов на пути пакета к получателю.

Протокол ICMP (Internet Control Message Protocol, Протокол Управляющих Сообщений Интернет) описан в RFC 792.
Он используется для сообщений об ошибках или нештатных ситуациях, передаваемых узлу-отправителю дейтаграммы узлом-получателем или промежуточным маршрутизатором.

Объединения сетей

Шлюзы

Сцепленные виртуальные каналы, дейтаграммное объединение и туннелирование



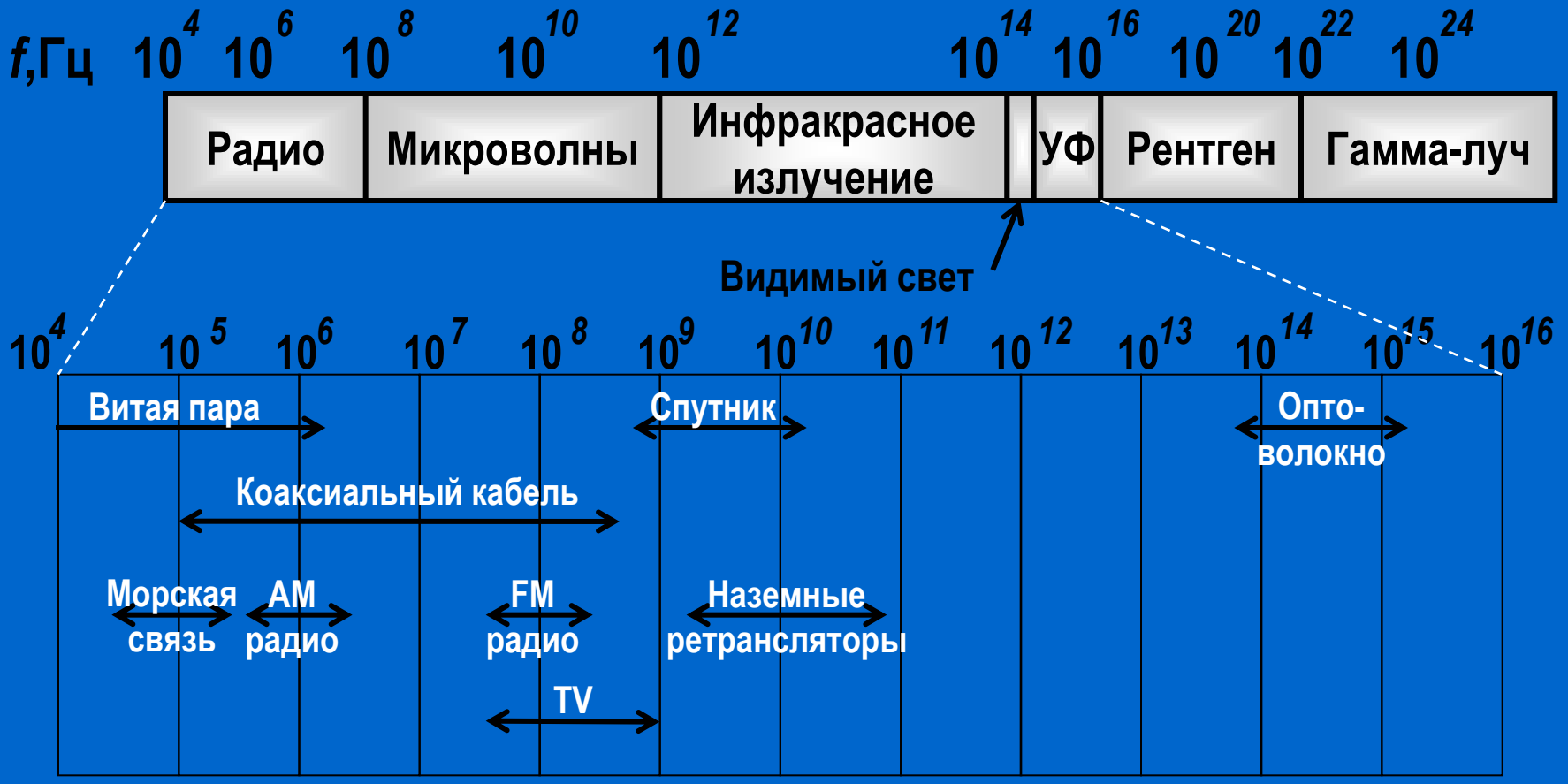
Оборудование сетей

Соответствие типов устройств и уровней

Тип устройства	Уровень модели OSI						
	Физический	Канальный	Сетевой	Транспортный	Сеансовый	Представления	Прикладной
Шлюз Gateway	+	+	+	+	+	+	+
Маршрутизатор Router	+	+	+				
Мост и коммутатор Bridge & Switch	+	+					
Повторитель и концентратор Repeator & Hub	+						

Тенденции развития сетей

Электромагнитный спектр



Современные технологии для телекоммуникаций

новые варианты "железа". К примеру, очень интересный вариант устройства - Communication Key: вместо "банального" UMTS-модема, в данной флэшке - "много-в-одном". По сути, это забавное развитие идеи Vonage - здесь "зашит" UMTS-модем и VoIP-клиент, причем по USB устройство можно подключить к любому компьютеру, оно само устанавливает соединение (предварительно проверяет, подключен ли компьютер к сети по проводному каналу или Wi-Fi) и включает VoIP-клиент, владелец может звонить. Причем, SIMка может быть от любого оператора. И выгодное отличие, которое позволяет эту штуку использовать в интернет-кафе и гостиничных компьютерах в бизнес-центре: она ничего не пишет на диск, все находится в оперативной памяти. Вытащил эту штуку из порта - и ПО самоликвидировалось, и ничего на жестком диске не осталось. А в памяти флэшки-модема в "боевом" режиме находится перезаписываемая память с новыми контактами, VoIP-логи соединений, логи IM-клиента и т.д. Гарнитура в комплекте и стоимость будет невелика - в районе 30-40 долл. Крайне вероятно, что с таких размеров и форм-фактора стартуют мобильные USB-модемы для сетей LTE

UMTS-сетей, так и для CDMA2000

Основным драйвером роста станут сети 3G – UMTS/HSPA, и дале

Популярная технология
DSL - Digital Subscriber Line

xDSL — семейство технологий, позволяющих значительно расширить пропускную способность абонентской линии местной телефонной сети путём использования эффективных линейных кодов и адаптивных методов коррекции искажений линии.

ADSL - ***Assimetric Digital Subscriber Line***
(ассиметричная цифровая абонентская линия)

VDSL - ***Very-high data rate Digital Subscriber Line***
(сверхвысокоскоростная цифровая абонентская линия)

ADSL

Сплиттер

ADSL-сплиттер разделяет частоты голосового сигнала (0,3 — 3,4 КГц) от частот, используемых ADSL-модемом (26 КГц — 1.4 МГц). Таким образом, исключается взаимное влияние модема и телефонного аппарата.

RJ-11:

Line (входящий)
Phone (выходящий)
Modem (выходящий)

Популярная технология xDSL

Технология xDSL	*Максимальная скорость (прием / передача)*	*Максимальное расстояние*
ADSL	24 Мбит/с / 3,5 Мбит/с	5,5 км
VDSL	65 Мбит/с / 35 Мбит/с	1,5 км на max. скорости

Популярная технология
На базе электропроводки

HomePlug - 14 Мбит/с
- 85 Мбит/с
HomePlug AV - 200 Мбит/с
HomePlug AV2 - июль 2010

Наложение на электрический ток (50 Гц) сигнала высокой частоты (от 1 до 30 МГц) со слабой энергией (менее 0,5 В).

Стандарт Home Plug

Home Plug Powerline Alliance включает (около 60 компаний):

- **Основатели Conexant, Cogency, Comcast, Earthlink, Panasonic и Sharp.**
- **Компании по производству технологических продуктов и электроники: Sony, Samsung, Motorola, Mitsubishi, MSI, Netgear и Belkin.**
- **Производители, которые желают воплощать в жизнь технологии, предложенные консорциумом HomePlug.**

На базе электропроводки

Адаптер Bewan Powerline E200 Duo

Характеристики Bewan Powerline E200 Duo	
Габариты	90 x 65 x 50 мм
Теоретическая пропускная способность	200 Мбит/с
Порты LAN	10/100 Мбит/с
Шифрование	3DES

На базе электропроводки

Адаптер Devolo dLan 200 AV

Характеристики Devolo dLan 200 AV	
Габариты	80 x 65 x 40 мм
Теоретическая пропускная способность	200 Мбит/с (22,3)
Порты LAN	10/100 Мбит/с
Шифрование	3DES

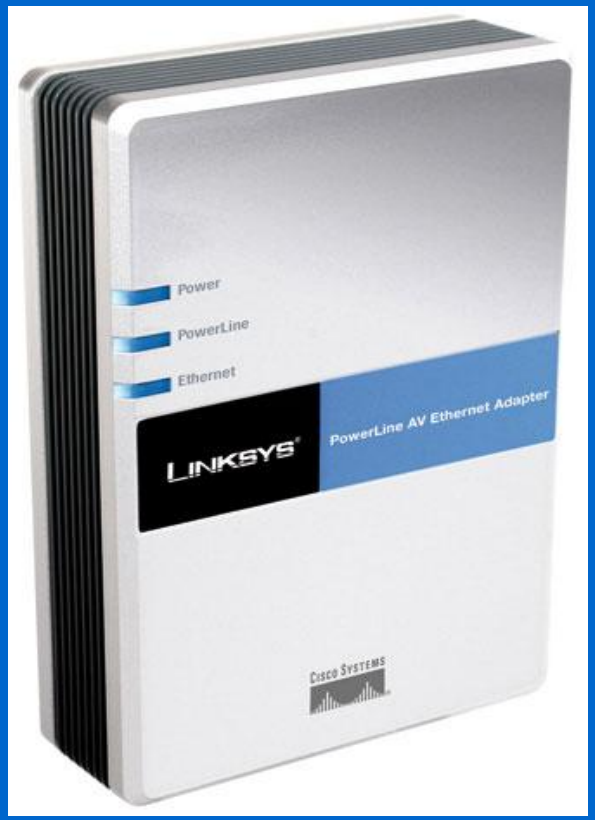
На базе электропроводки

Адаптер D-Link DHP-301

Характеристики D-Link DHP-301	
Габариты	105 x 75 x 40 мм
Теоретическая пропускная способность	200 Мбит/с
Порты LAN	10/100 Мбит/с
Шифрование	3DES

На базе электропроводки

Адаптер Linksys PLK200



Характеристики Linksys PLK200	
Габариты	140 x 100 x 50 мм
Теоретическая пропускная способность	200 Мбит/с
Порты LAN	10/100 Мбит/с
Шифрование	3DES

На базе электропроводки

Адаптер Olitec CPL200

Характеристики Olitec CPL200	
Габариты	115 x 70 x 40 мм
Теоретическая пропускная способность	200 Мбит/с
Порты LAN	10/100 Мбит/с
Шифрование	3DES

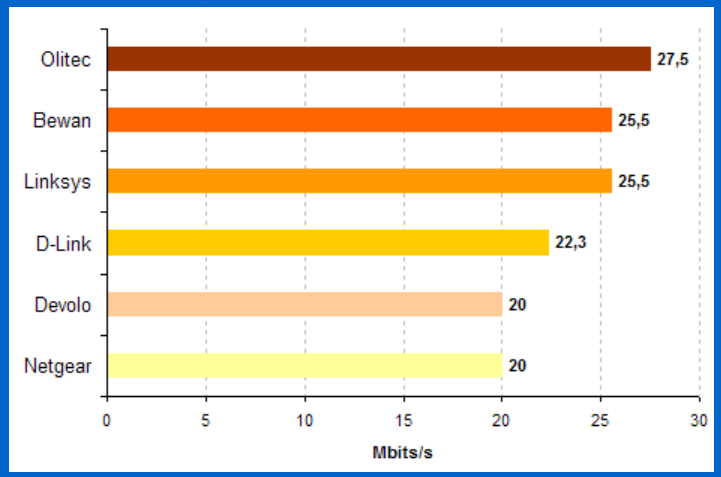
На базе электропроводки

Адаптер Netgear HDX101

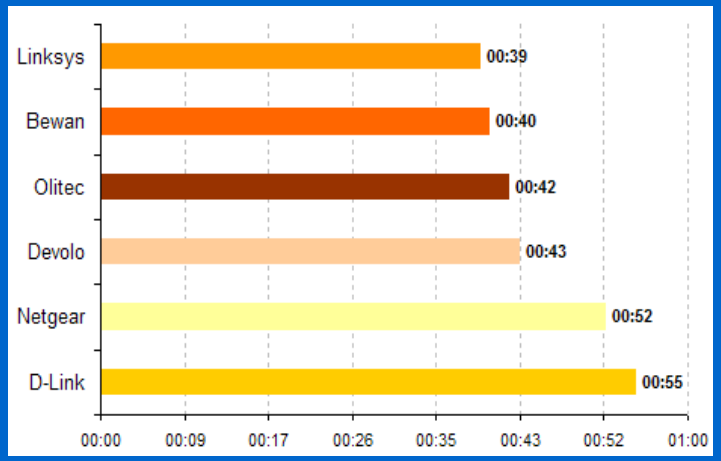
Характеристики Netgear HDX101	
Габариты	97 x 71 x 40 мм
Теоретическая пропускная способность	200 Мбит/с
Порты LAN	10/100 Мбит/с
Шифрование	3DES

Популярные технология на базе электропроводки (сравнение)

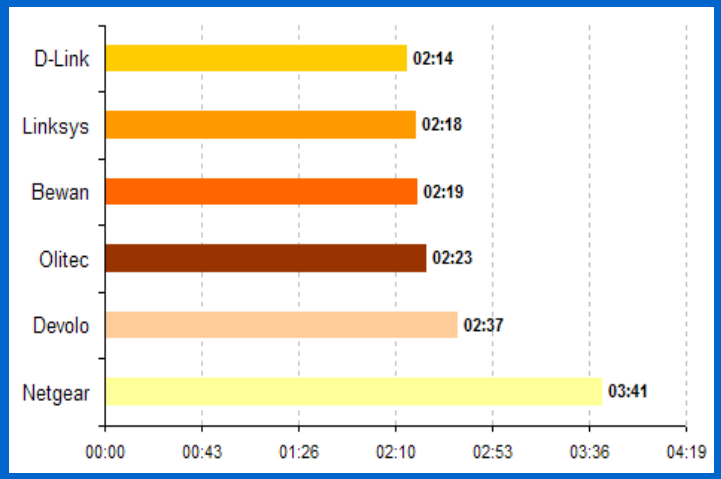
Скорость потока, Мбит/с.



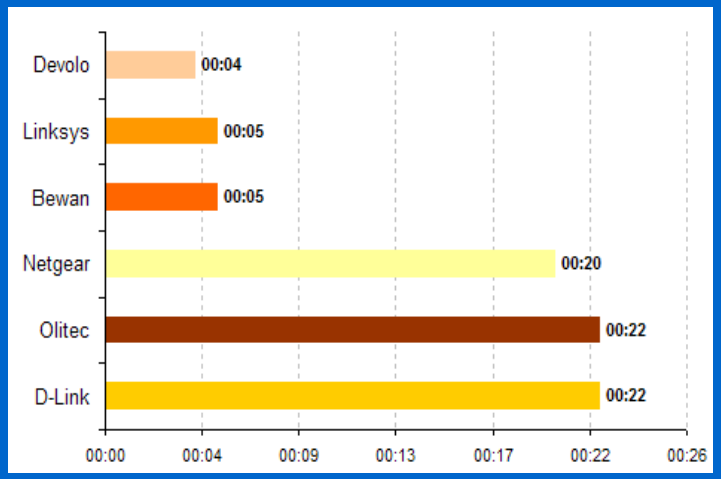
Время передачи файла в 100 Мбайт



Время передачи файла в 700 Мбайт

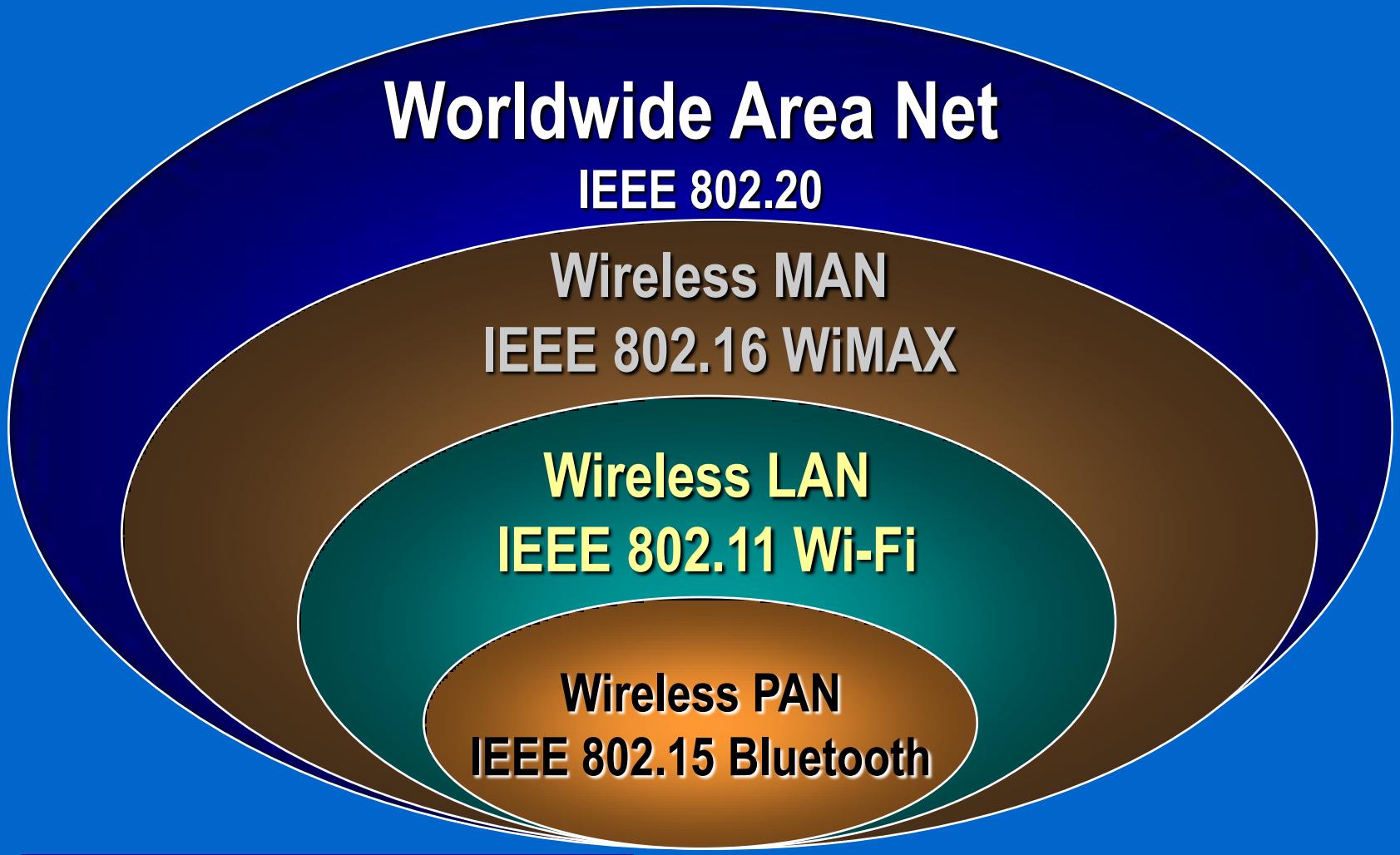


Время синхронизации, секунды



Тенденции развития сетей

Беспроводные сети



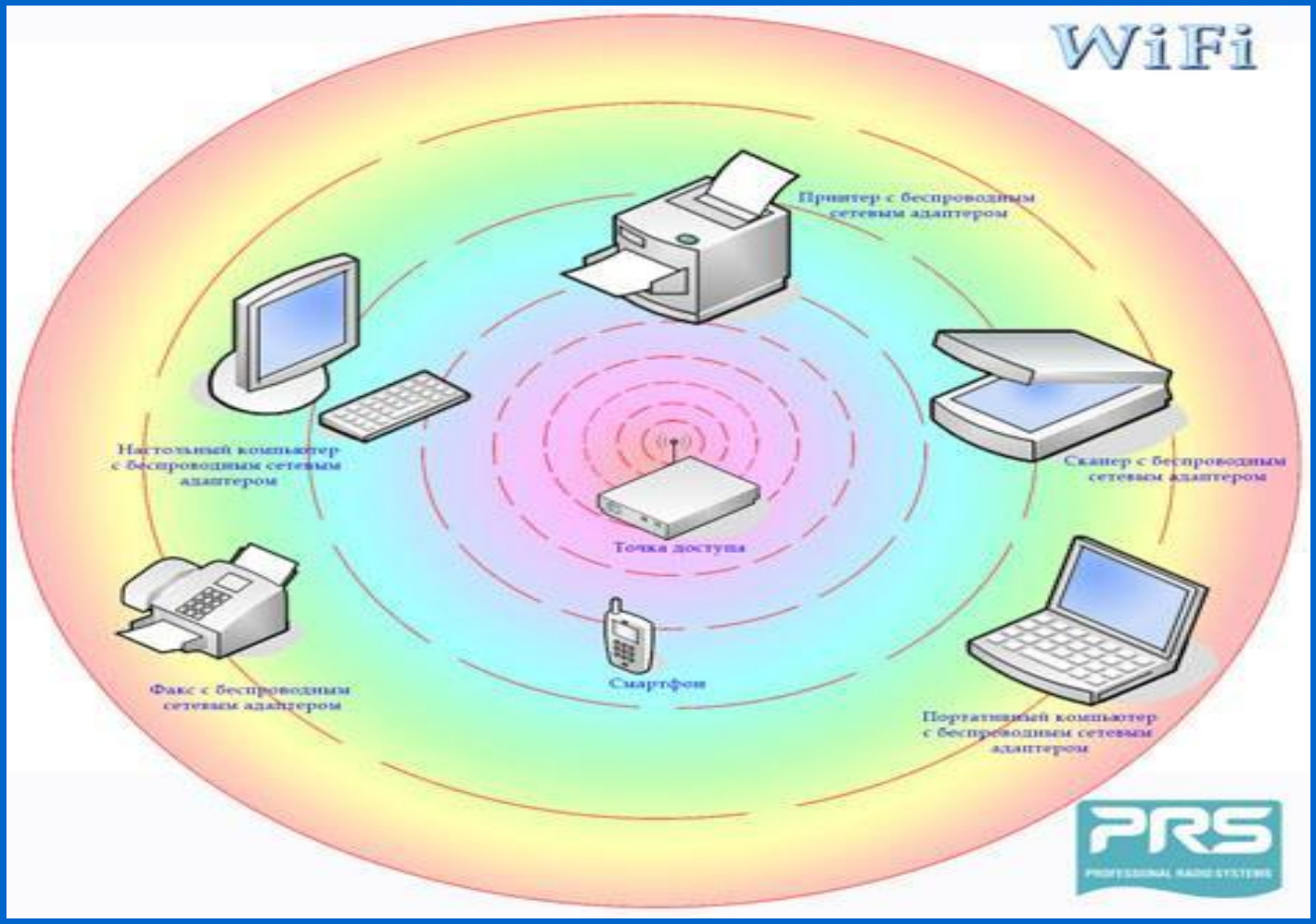
Беспроводные PAN

Bluetooth, UMB, ZigBee, IrDa

Технология	*Стандарт*	*Использо-вание*	*Скорость (Мбит/с)*	*Радиус действия*	*Частота*
Bluetooth v. 1.1.	802.15.1	WPAN	до 1 Мбит/с	до 10 метров	2,4 ГГц
Bluetooth v. 1.3.	802.15.3	WPAN	11- 55 Мбит/с	до 100 метров	2,4 ГГц
ZigBee	802.15.4	WPAN	20 - 250 Кбит/с	1-100 м	2,4 ГГц (16кан) 915 МГц (10 кан) 868 МГц (1 кан)
UWB	802.15.3a	WPAN	110 - 480 Мбит/с	до 10 метров	7,5 ГГц
Инфракрасный порт	IrDa	WPAN	115,2 Кбит/с	от 5 до 50 сантиметров, односторонняя связь — до 10 метров	

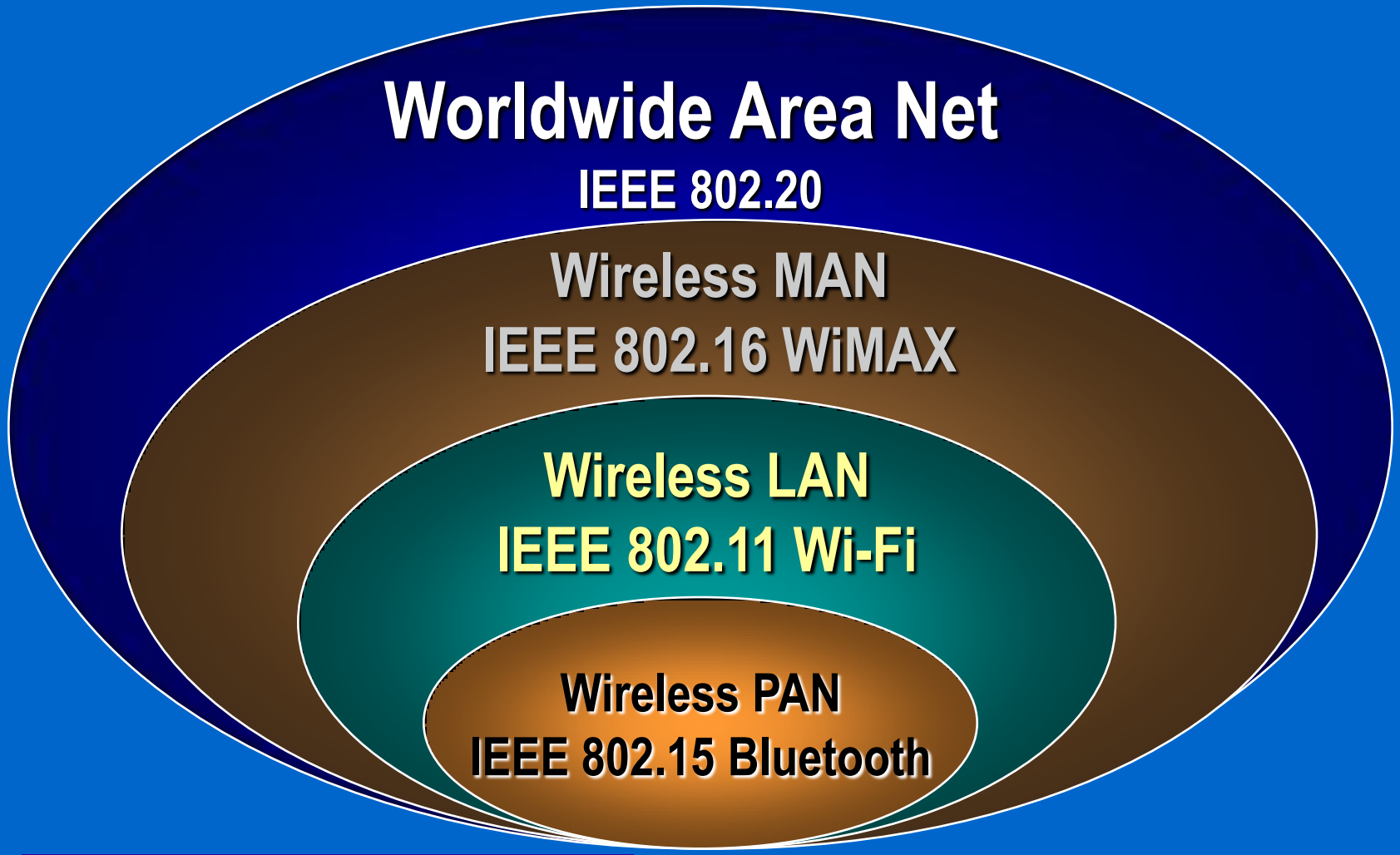
Тенденции развития сетей

Беспроводные сети (802.11 – Wi-Fi)



Тенденции развития сетей

Беспроводные сети



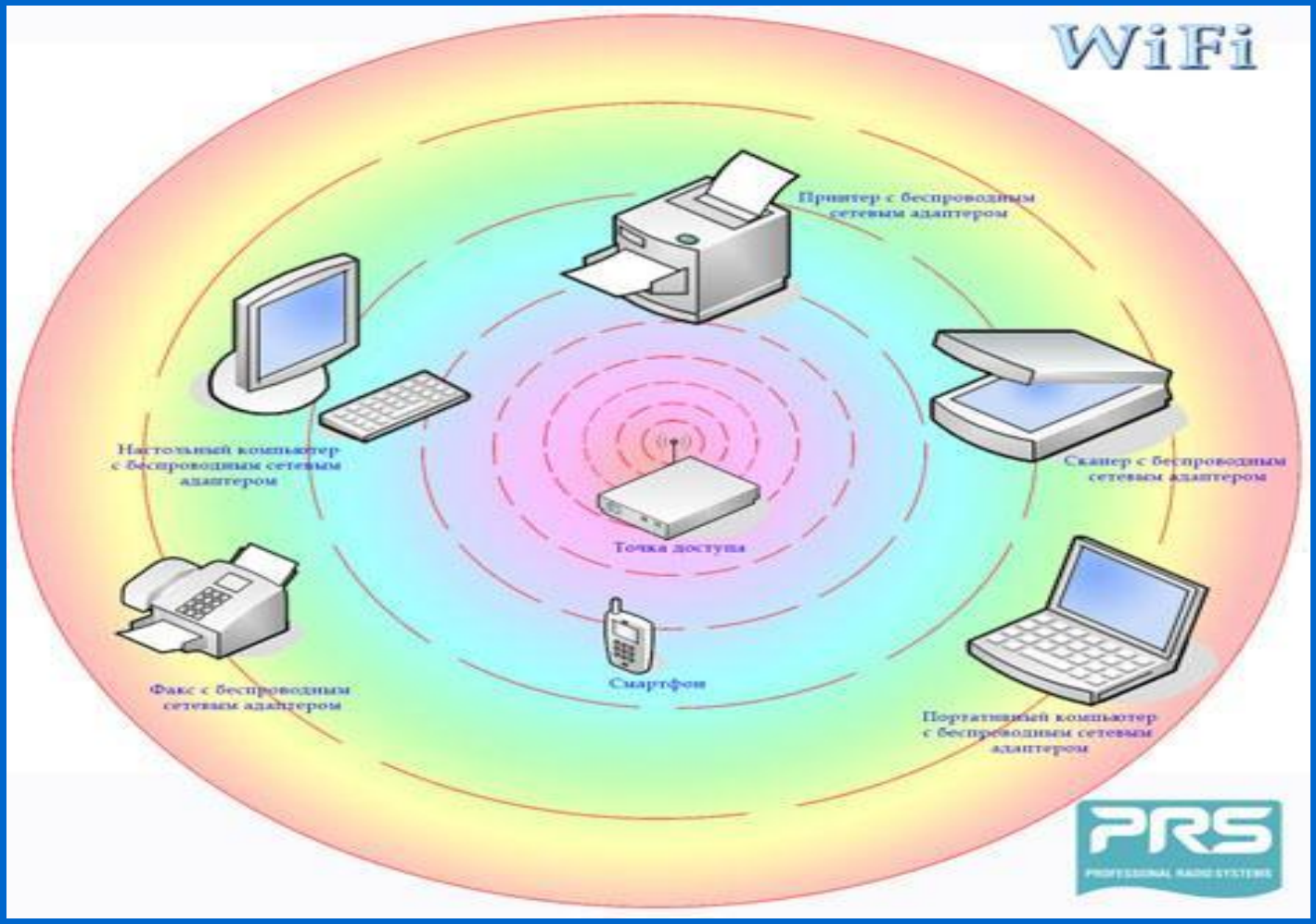
Беспроводные PAN

Bluetooth, UMB, ZigBee, IrDa

Технология	*Стандарт*	*Использо-вание*	*Скорость (Мбит/с)*	*Радиус действия*	*Частота*
Bluetooth v. 1.1.	802.15.1	WPAN	до 1 Мбит/с	до 10 метров	2,4 ГГц
Bluetooth v. 1.3.	802.15.3	WPAN	11- 55 Мбит/с	до 100 метров	2,4 ГГц
ZigBee	802.15.4	WPAN	20 - 250 Кбит/с	1-100 м	2,4 ГГц (16кан) 915 МГц (10 кан) 868 МГц (1 кан)
UWB	802.15.3a	WPAN	110 - 480 Мбит/с	до 10 метров	7,5 ГГц
Инфракрасный порт	IrDa	WPAN	115,2 Кбит/с	от 5 до 50 сантиметров, односторонняя связь — до 10 метров	

Тенденции развития сетей

Беспроводные сети (802.11 – Wi-Fi)



Беспроводные LAN

Wi-Fi

Техно-логия	Стандарт	Использо-вание	Скорость (Мбит/с)	Радиус действия (м)	Частота (ГГц)
Wi-Fi	802.11a	WLAN	54	до 100	5,0
Wi-Fi	802.11b	WLAN	11	до 100	2,4
Wi-Fi	802.11g	WLAN	108	до 100	2,4
Wi-Fi	802.11n	WLAN	600	до 100	2,4 —5,0

Область использования

WiMAX подходит для решения следующих задач:

- Соединения точек доступа Wi-Fi друг с другом и другими сегментами Интернета.
- Обеспечения беспроводного широкополосного доступа как альтернативы выделенным линиям и DSL.
- Предоставления высокоскоростных сервисов передачи данных и телекоммуникационных услуг.
- Создания точек доступа, не привязанных к географическому положению.

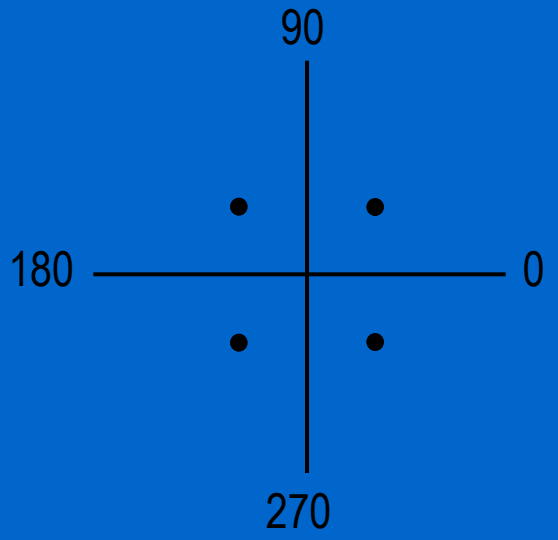
Тенденции развития сетей

Широкополосные беспроводные сети (802.16)

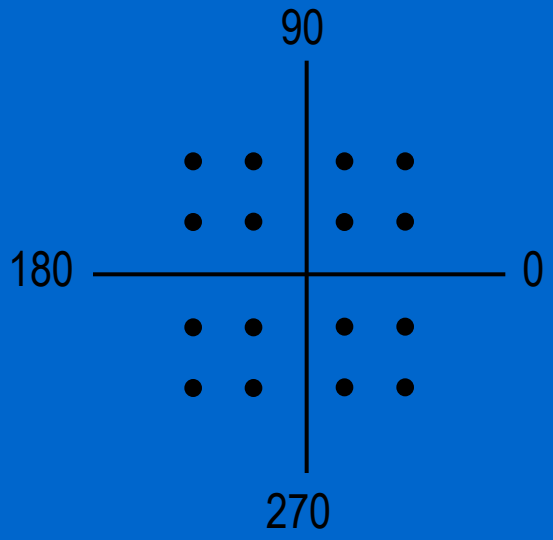
Диапазон 10- 66 Ггц (миллиметровые волны), типичная полоса спектра 25 Мгц

QPSK – Quadrature Phase Shift Keying – квадратурная фазовая манипуляция

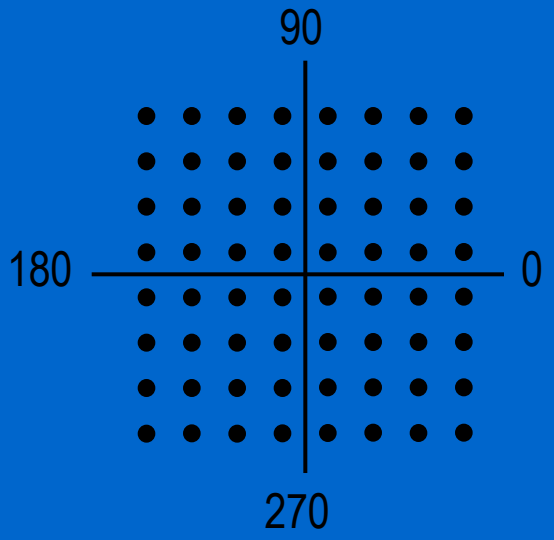
QAM - Quadrature Amplitude Modulation – квадратурная амплитудная модуляция



QPSK
50 Мбит/сек



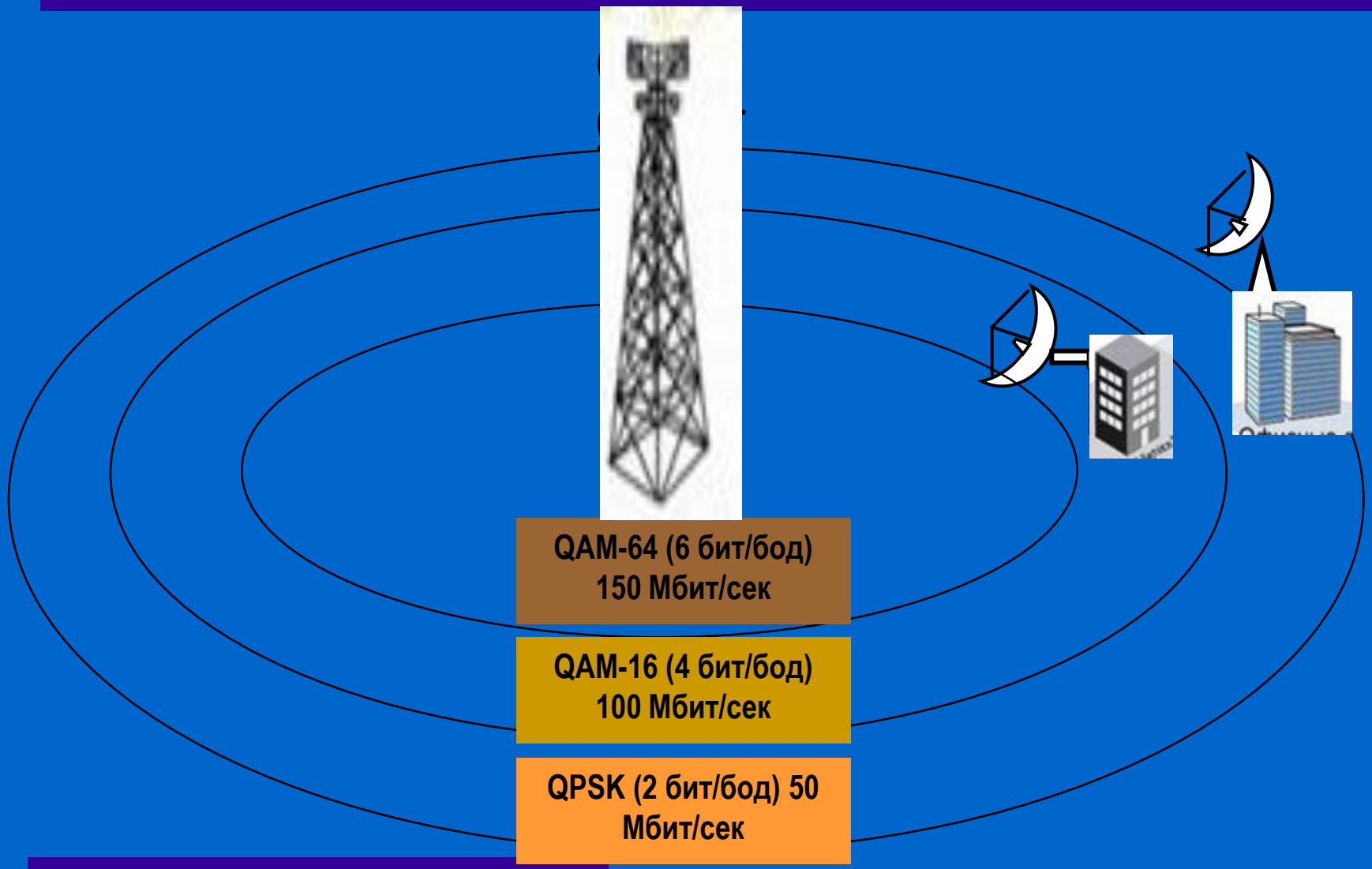
QAM-16
100 Мбит/сек



QAM-64
150 бит/сек

Тенденции развития сетей

Широкополосные беспроводные сети



WiMAX

802.16d - фиксированный

Спецификация утверждена в 2004 году. Используется ортогональное частотное мультиплексирование (OFDM), поддерживается фиксированный доступ в зонах с наличием либо отсутствием прямой видимости.

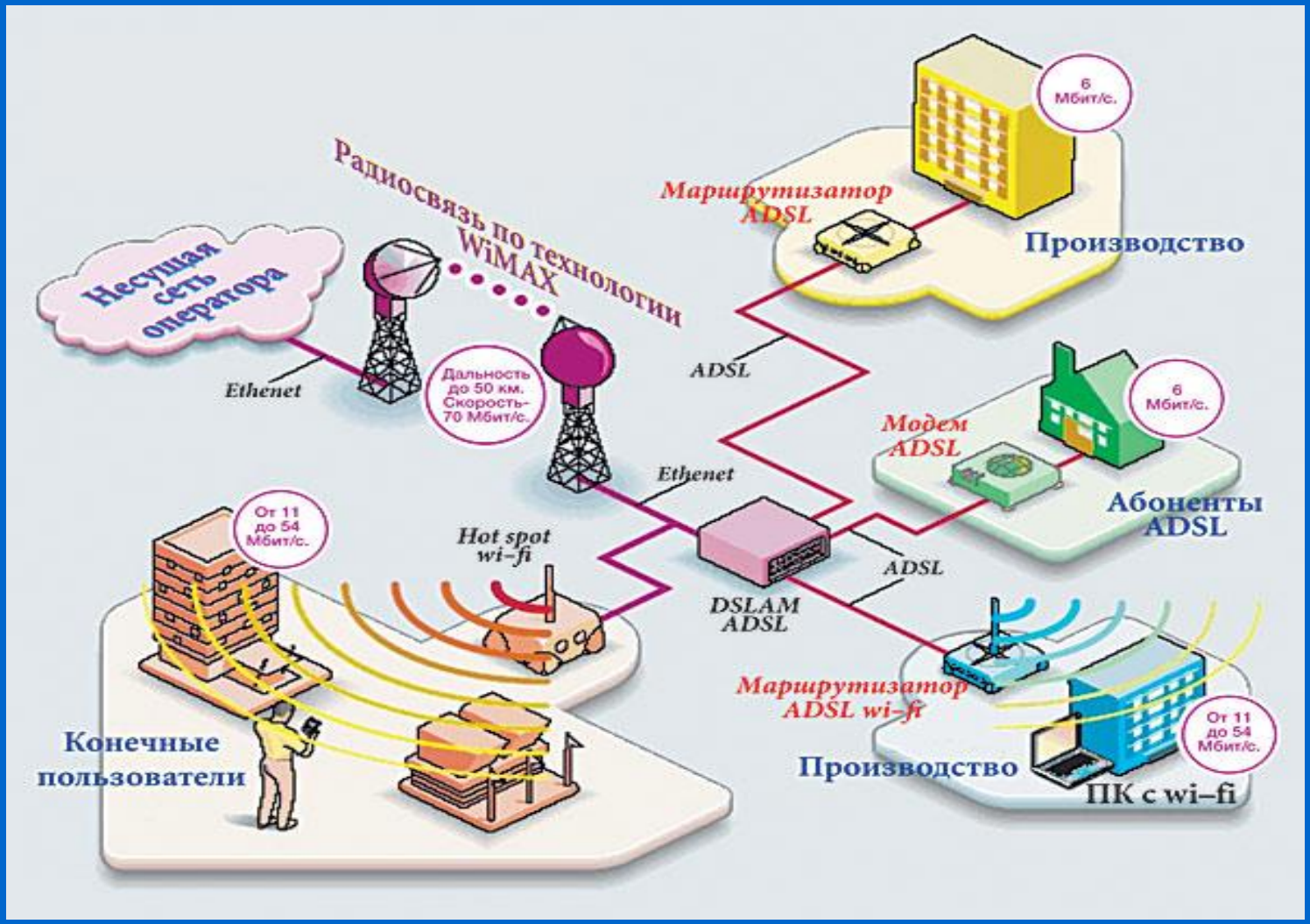
Пользовательские устройства представляют собой стационарные модемы для установки вне и внутри помещений, а также PCMCIA-карты для ноутбуков.

В большинстве стран под эту технологию отведены диапазоны 3,5 и 5 ГГц. По сведениям WiMAX Forum, насчитывается уже порядка 175 внедрений фиксированной версии.

Многие аналитики видят в ней конкурирующую или взаимодополняющую технологию проводного широкополосного доступа DSL.

Тенденции развития сетей

Широкополосные беспроводные сети (WiMAX)



WiMAX

802.16e – мобильный

Спецификация утверждена в 2005 году. Это — новый виток развития технологии фиксированного доступа (802.16d).

Оптимизированная для поддержки мобильных пользователей версия поддерживает ряд специфических функций, таких как хэндовер(англ.), *idle mode* и роуминг. Применяется масштабируемый OFDM-доступ (SOFDMA), возможна работа при наличии либо отсутствии прямой видимости.

Планируемые частотные диапазоны для сетей Mobile WiMAX таковы: 2,3-2,5; 2,5-2,7; 3,4-3,8 ГГц. В мире реализованы несколько пилотных проектов, в том числе первым в России свою сеть развернул «Скартел».

Конкурентами 802.16e являются все мобильные технологии третьего поколения (например, EV-DO, HSDPA).

Тенденции развития сетей

Широкополосные беспроводные сети (WiMAX)

Беспроводные MAN

WiMAX

Техно-логия	*Стандарт*	*Использование*	*Скорость (Мбит/с)*	*Радиус действия*	*Частота (ГГц)*
WiMax	802.16d	WMAN	до 75	6-10 км	1,5-11
WiMax	802.16e	Mobile WMAN	до 30	1-5 км	2-6
WiMax	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	н/д	н/д

Тенденции развития сетей

Широкополосные беспроводные сети (802.16)

Полосой пропускания среды называется диапазон частот, которые могут передаваться в этой среде с минимальным затуханием.

Скорость двоичной передачи (в бодах) – это число отсчетов, совершаемых за одну секунду. Каждый отсчет передает единицу информации – символ. Скорость двоичной передачи равна скорости передачи символов. Метод модуляции определяет число бит, из которых состоит один символ.

Битовой скоростью называется объем информации, передаваемый по каналу за секунду. Битовая скорость равна произведению числа символов в секунду и числа бит на символ (символ/сек х бит/символ).

Службы и протоколы Интернета

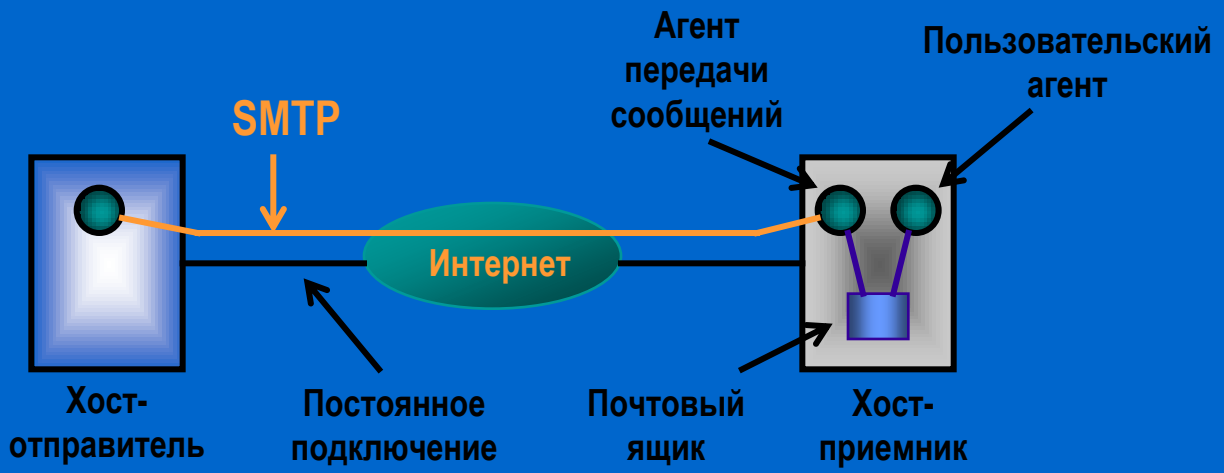
SMTP, POP3, FTP, UDP, RTP, HTTP

- Электронная почта (SMTP, POP3)
- Пересылка файлов (FTP, UDP, RTP)
- Всемирная паутина (HTTP)

Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- Электронная почта (SMTP)

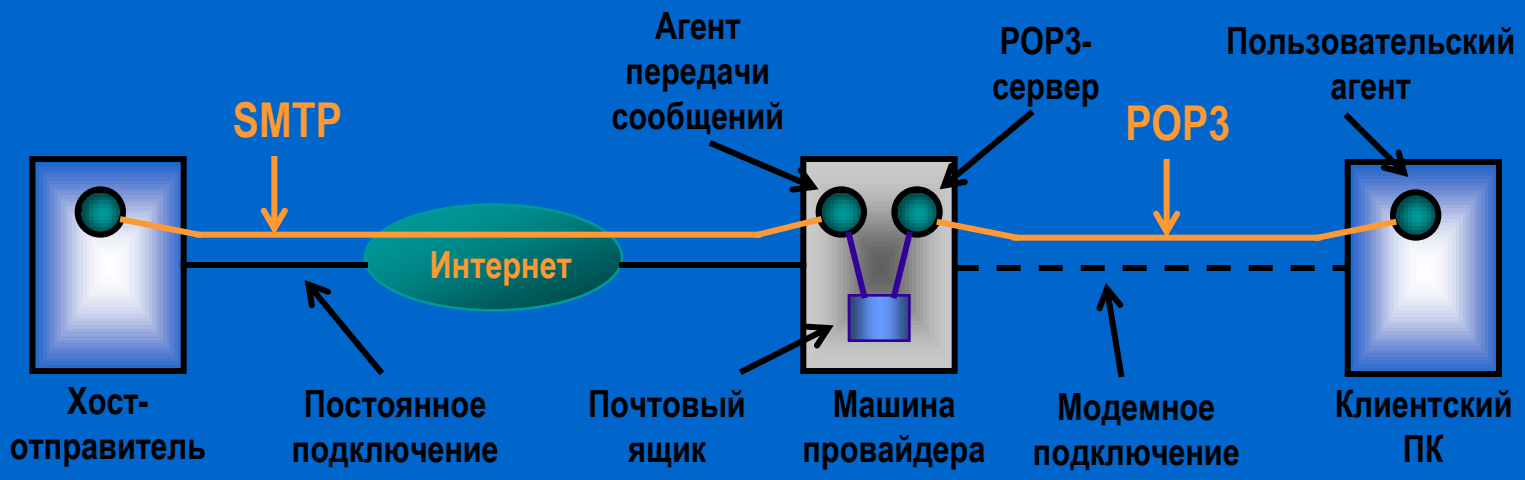


TCP-соединение с портом 25 хоста-приемника
Хост-отправитель – клиент, хост-приемник - сервер

Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- Электронная почта (SMTP,POP3)



TCP-соединение с портом 110 агента передачи сообщений
Машина провайдера – сервер, клиентский ПК – клиент:

1. Авторизация, 2. Транзакции, 3. Обновление

Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- **Электронная почта (POP3)**

1. Авторизация, 2. Транзакции, 3. Обновление

telnet (DNS-имя провайдера) 110

S: +OK POP3-сервер готов
C: USER …
S: +OK
C: PASS …
S: OK вход в систему произведен
C: LIST
S: 1 2678
S: 254906
S: .

C: RETR 1
S: (отправляет сообщение 1)
C: DELE 1
C: RETR 2
S: (отправляет сообщение 2)
C: DELE 2
C: QUIT
S: +OK Конец соединения

Электронная почта

Смайлики или эмотиконы

:-) Не воспринимай всерьез	=:-) Г-н Линкольн	:+) Большой нос
:-(Я зол / огорчен	=):=) Дядя Сэм	:-)) Двойной подбородок
:-| Мне это безразлично	*<:-) Дед мороз (Клоун)	:-{) С усами
;-) Подмигиваю	<:-(Болван	#:-) Взъерошенные волосы
:(O) Громко кричу	(-: Австралиец (левша)	8-) Носит очки
:-(*) Мне от этого тошно	:-)X С бабочкой	C:-) Очень умный

Жаргон: BTW - By The Way

ROTFL – Rolling On The Floor Laughing

IMHO – In My Humble Opinion

Sanderson, Dougherty 1993 (>650)

Электронная почта

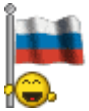
Смайлики или эмотиконы

http://smiles2k.net

Музыкальные 

Для админов 

Рождественские 

Национальные 

Спортивные 

Большие 

С компьютером 

Прыгающие 

Курящие 

Крутые 

Боевые 

Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- Передача файлов (FTP)

В основе TCP – сокеты, гнезда или конечные точки обменивающихся хостов. Номер (адрес) сокета – IP-адрес хоста + 16-битный номер порта.

Номера портов ниже 1024 – популярные, зарезервированы сервисами.

Например: FTP-передача – порт 21. Список портов: *www.iana.org* (>300)

Порт	Протокол	Использование
21	FTP	Передача файлов
23	Telnet	Дистанционный вход в систему
25	SMTP	Электронная почта
69	TFTP	Простейший протокол передачи данных
79	Finger	Поиск информации о пользователе
80	HTTP	Мировая паутина (гипертексты)
110	POP-3	Удаленный доступ к электронной почте
119	NNTP	Группы новостей

Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- **Передача файлов (UDP)**

Пользовательский дейтаграммный протокол – обслуживает отправку инкапсулированных IP-дейтаграмм без установления соединений.

UDP описан в RFC 786.

Заголовок UDP – 32 бита

Порт источника	Порт назначения
Длина UDP	Контрольная сумма UDP

UDP не занимается контролем потока, контролем ошибок, повторной передачей после приема испорченного пакета. Этим должен заниматься пользовательский процесс. UDP широко используется в:

- **Клиент-серверные приложения**
- **Служба имен доменов (DNS)**

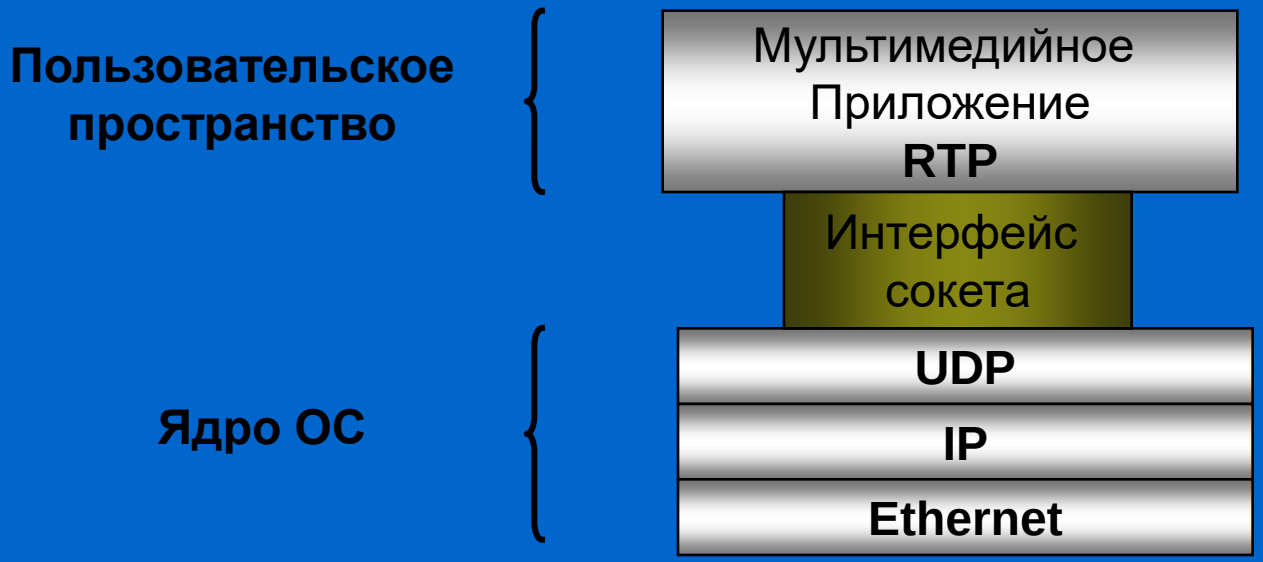
Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- Передача файлов (RTP)

RTP – Real-Time Transport Protocol - транспортный протокол реального масштаба времени – обслуживает отправку мультимедиа.

RTP описан в RFC 1889.



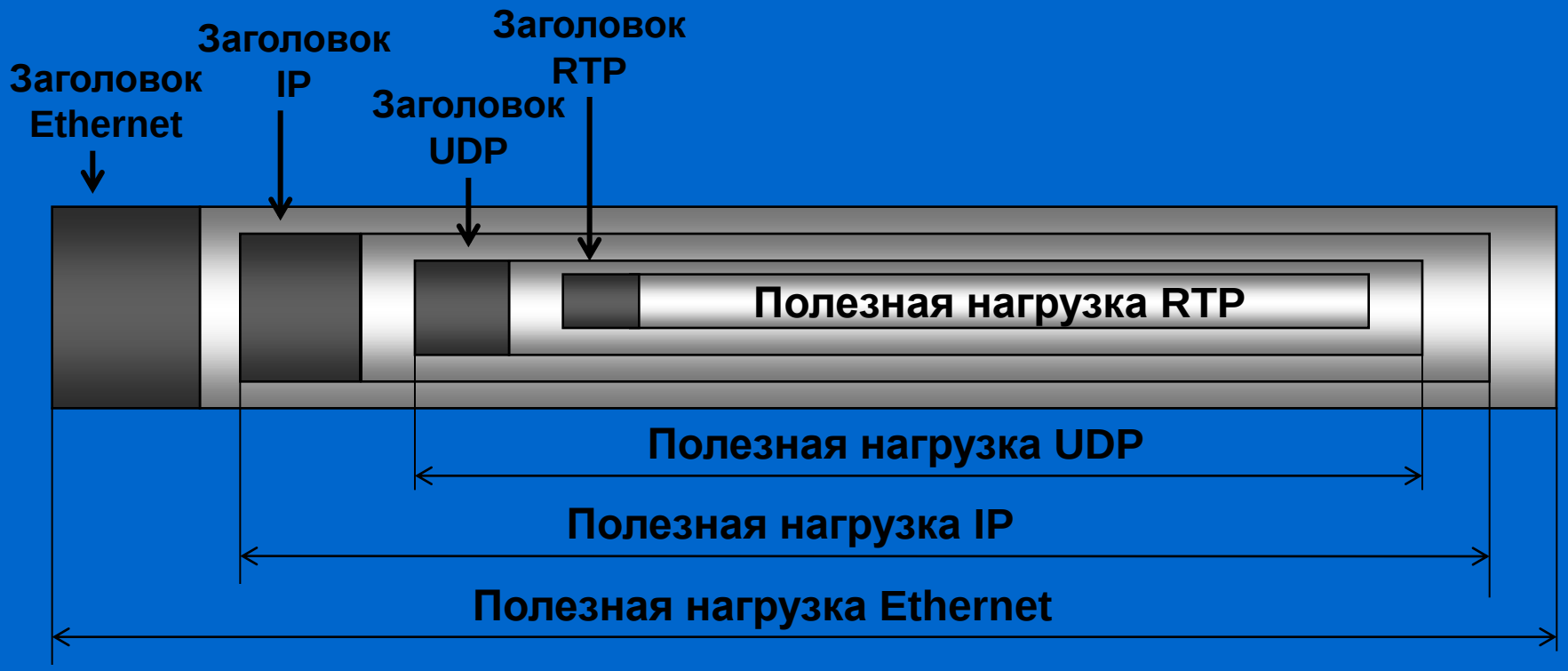
Основная функция RTP – уплотнение нескольких потоков реального масштаба времени в единый поток пакетов UDP.

Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- Передача файлов (RTP)

Профили – отдельные медиапотоки, каждый со своей кодировкой (GSM, MP3, дельта-кодирование и т.п.). В заголовке – отметка времени.



Службы и протоколы Интернета

SMTP, POP3, FTP, UDP, RTP, HTTP

- **Всемирная паутина (HTTP)**

Программа, принимающая запросы от пользователей и выдающая им файлы, называется *Web-сервером*. Этим термином также именуют компьютер, где она работает. Иногда, чтобы не было путаницы, дополнительно уточняют, что имеется в виду: компьютер или программа.

Пользователь запрашивает Web-страницы, набирая в поле адреса Web-обозревателя адрес страницы:

- http://www.microsoft.com — адрес сайта Microsoft.
- http://www.netscape.com — а это адрес Netscape.
- http://www.music.ru — огромная база данных русских музыкальных исполнителей.

WEB программирование

Cookies

Cookie является решением одной из наследственных проблем ***HTTP*** протокола (Hyper Text Transfer Protocol). Эта проблема заключается в непостоянстве соединения между клиентом и сервером, как при ***FTP*** или ***Telnet*** сессии.

Для каждого документа (или файла) при передаче по HTTP протоколу посылается отдельный запрос. Включение ***cookie*** в ***HTTP*** протокол дает частичное решение этой проблемы: транзакция завершается после того, как браузер сделал запрос, а сервер выдал соответствующий ответ.

Сразу после этого сервер "забывает" о пользователе и каждый следующий запрос того же пользователя считает запросом нового пользователя.

WEB программирование

Cookies *(продолжение)*

Cookie позволяет эмулировать сессию по HTTP протоколу: на первом запросе выдается соответствующее значение cookie, а при каждом последующем запросе это значение читается из переменной окружения ***HTTP_COOKIE*** и соответствующим образом обрабатывается.

Пример: есть форма, где пользователю предлагается указать свое имя, из нее вызывается скрипт, который прописывает значение cookie в браузер пользователя. При каждом последующем заходе на основе анализа значения cookie из браузера пользователя на странице появляется либо именное приветствие (если есть установленное значение cookie), либо первоначальная форма с запросом имени пользователя (если значение cookie не установлено).

WEB программирование

Cookies *(продолжение)*

Cookie - это небольшая порция текстовой информации, которую сервер передает браузеру. Браузер будет хранить эту информацию и передавать ее серверу с каждым запросом как ***часть HTTP заголовка***.

Одни значения cookie могут храниться только в течение одной сессии, они удаляются после закрытия броузера. Другие, установленные на некоторый период времени, записываются в файл. Обычно этот файл называется ***cookies.txt*** и лежит в рабочей директории установленного на компьютер браузера.

Язык HTML

Cookies *(компоненты)*

Имя — имя cookie является обязательным параметром, по которому программа ссылается на cookie. Можно провести аналогию между именем cookie и именем переменной.

Значение — фрагмент данных, связанный с именем cookie. В этих данных может храниться любая информация — идентификатор пользователя, цвет фона, текущая дата и т. д.

Срок действия — дата, определяющая продолжительность существования cookie. Согласно спецификации, если срок действия не указан, cookie становится недействительным в конце сеанса (то есть когда пользователь покидает сайт).

Домен — домен, который создал cookie и может читать его значение.

Путь — URL, с которого предоставляется доступ к cookie. Любые попытки получения доступа к cookie за пределами этого пути пресекаются. Данный компонент необязателен; если он не задан, по умолчанию используется путь к документу, создавшему cookie.

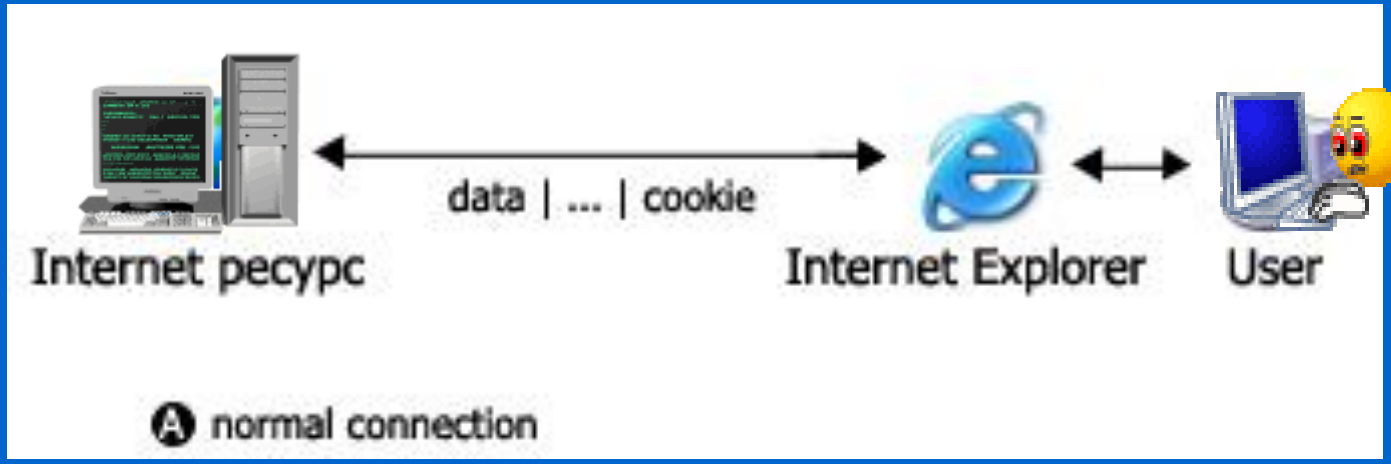
Безопасность — параметр, показывающий, допускается ли чтение cookie в небезопасной среде. По умолчанию используется значение FALSE.

Хотя при создании cookie используются одни и те же синтаксические правила, формат хранения cookie зависит от браузера.

Язык HTML

Cookies *(продолжение)*

Set-Cookie: *NAME*=value; *EXPIRES*=date; *DOMAIN*=domain_name; *PATH*=path; *SECURE*



Язык HTML

Cookies *(ограничения)*

Клиент (браузер) имеет следующие ограничения для cookies:

- всего может храниться ***до 300 значений*** cookies
- каждый cookie не может превышать ***4Кбайт***
- с одного сервера или домена может храниться ***до 20 значений*** cookie

Если ограничение ***300 или 20 превышается***, то удаляется первая по времени запись.

При превышении лимита объема в ***4Кбайт*** корректность значения cookie страдает - отрезается кусок записи (с начала этой записи) равный превышению объема.

Язык HTML

Cookies *(функция установки)*

```
function setCookie(name, value, expires, path, domain, secure) {
      var curCookie = name + "=" + escape(value) +
          ((expires) ? "; expires=" + expires.toGMTString() : "") +
          ((path) ? "; path=" + path : "") +
          ((domain) ? "; domain=" + domain : "") +
          ((secure) ? "; secure" : "")
     if (!caution || (name + "=" + escape(value)).length <= 4000)
          document.cookie = curCookie
     else
          if (confirm("Cookie превышает 4KB и будет вырезан !"))
              document.cookie = curCookie
}
```

Язык HTML

Cookies *(функция чтения)*

Возвращает установленное значение или пустую строку, если cookie не существует.

```
// name - имя считываемого cookie
function getCookie(name) {
        var prefix = name + "="
        var cookieStartIndex = document.cookie.indexOf(prefix)
        if (cookieStartIndex == -1)
            return null
        var cookieEndIndex = document.cookie.indexOf(";",
                                cookieStartIndex + prefix.length)
        if (cookieEndIndex == -1)
            cookieEndIndex = document.cookie.length
        return unescape(document.cookie.substring
                (cookieStartIndex + prefix.length, cookieEndIndex))
}
```

Язык HTML

Cookies *(функция удаления)*

Принцип работы этой функции заключается в том, что cookie устанавливается с заведомо устаревшим параметром expires, в данном случае 1 января 1970 года.

```
// name - имя cookie
// [path] - путь, для которого cookie действительно
// [domain] - домен, для которого cookie действительно

function deleteCookie(name, path, domain) {
        if (getCookie(name)) {
            document.cookie = name + "=" +
            ((path) ? "; path=" + path : "") +
            ((domain) ? "; domain=" + domain : "") +
            "; expires=Thu, 01-Jan-70 00:00:01 GMT"
          }
}
```

Расширение HTML

Язык VBScript

Языки сценария, такие как Java Script и VBScript, созданы как расширение для HTML. Браузер получает сценарий вместе с остальной частью Web-страницы, именно браузер должен проанализировать и выполнить сценарий. Для внедрения сценария на страницу в HTML служит тэг **<SCRIPT>** и **</SCRIPT>**.

```
<HTML>
 <HEAD> <TITLE>Работа в VBScript: Упражнение 1</TITLE> </HEAD>
  <BODY>
  <H1>Пример работы в VBScript</H1>
  <P>Первое упражнение. Нажмите на кнопку для получения
сообщения.</P>
       <FORM name="frmExercise1">
                  <INPUT TYPE="Button" Name="cmdClickMe" VALUE="Нажми
меня">
                  <SCRIPT FOR="cmdClickMe" EVENT="onClick"
LANGUAGE="VBSCRIPT">
                   MsgBox "Добро пожаловать на мою страницу!"
                  </SCRIPT>
       </FORM>
  </BODY>  </HTML>
```

Язык VBScript

Вставка сценария на VBScript на страницу

```
<HTML>
<HEAD>
<TITLE>Работа в VBScript: Упражнение 1</TITLE>
</HEAD>
<BODY>
  <H1>Пример работы в VBScript</H1>
  <P>Это первое упражнение по работе в VBScript. Нажмите
    на кнопку для получения сообщения.</P>
  <FORM name="frmExercise1">
    <INPUT TYPE="Button" Name="cmdClickMe" VALUE="Нажми меня">
  </FORM>
</HEAD>
</HTML>
```

Безопасность в сетях

Типы нарушителей и цели их действий

Студент	Прочитать из любопытства чужие письма
Хакер	Проверить на прочность чужую систему безопасности, украсть данные
Торговый агент	Притвориться представителем всей Европы, а не только Андорры
Бизнесмен	Разведать стратегические маркетинговые планы конкурента
Уволенный сотрудник	Отомстить фирме за увольнение
Бухгалтер	Украсть деньги компании
Биржевой брокер	Не выполнить обещание, данное клиенту по электронной почте
Аферист	Украсть номера кредитных карт для продажи
Шпион	Узнать военные или производственные секреты противника
Террорист	Украсть секреты производства оружия

Безопасность в сетях

Аспекты безопасности

Секретность - (конфиденциальность) предотвращение попадания информации в руки неавторизованных пользователей.

Аутентификация - позволяет определить, с кем вы имеете дело, прежде чем предоставить собеседнику доступ к секретной информации или вступить с ним в деловые отношения.

Обеспечение строгого выполнения обязательств - имеет дело с подписями.

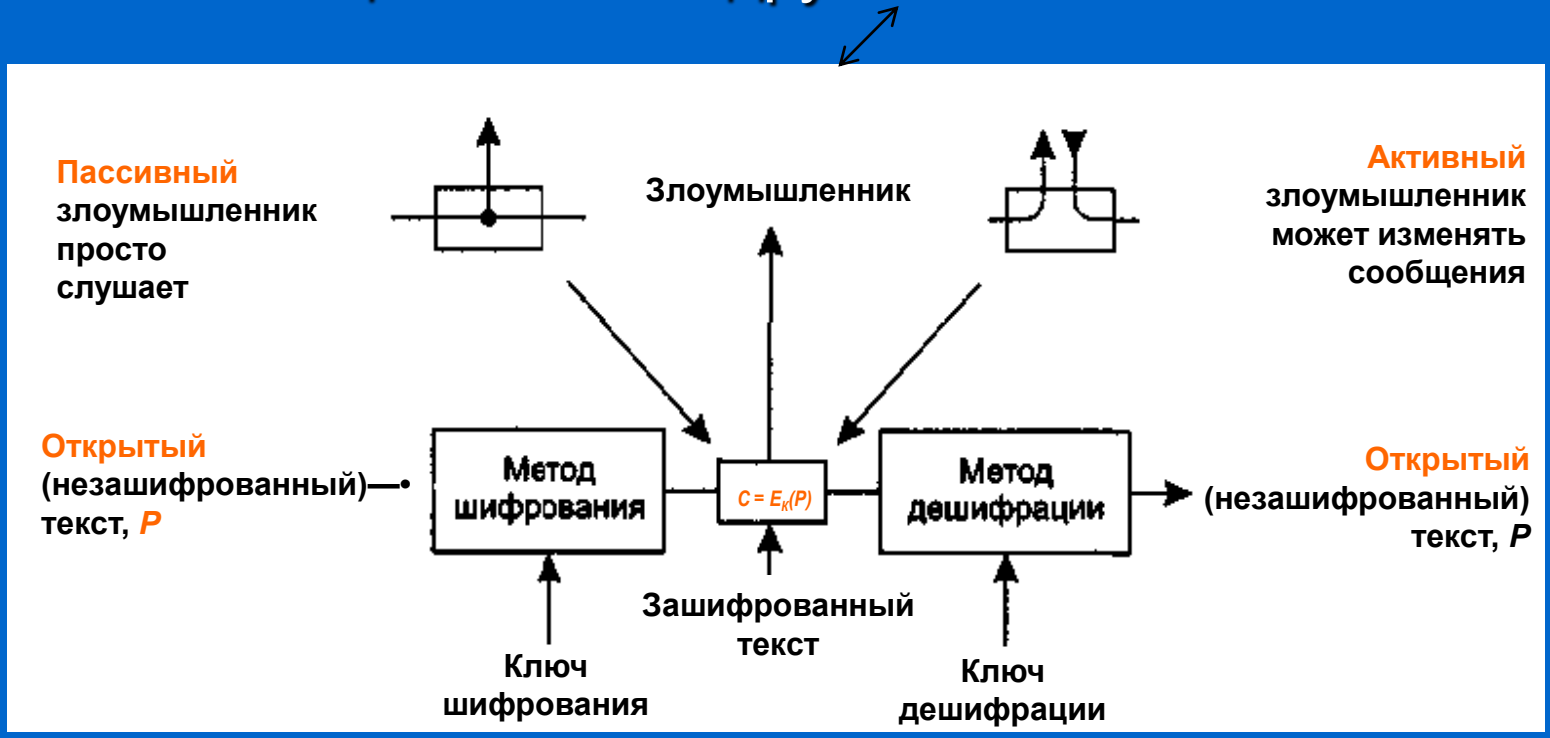
Обеспечение целостности - позволяет быть уверенным, что принятое сообщение не подделано и не изменено по пути злоумышленником.

Безопасность в сетях

Основы криптографии

Шифр - посимвольное или побитовое преобразование, не зависящее от лингвистической структуры сообщения.

Код - заменяет целое слово другим словом или символом.



Безопасность в сетях

Основы криптографии

Искусства изобретать шифры (**криптография**) и взламывать их (**криптоанализ**) называются вместе **криптологией**.

$C = E_K(P)$ - при зашифровке открытого текста P с помощью ключа K получается зашифрованный текст C.

$P = D_K(C)$ - означает расшифровку зашифрованного текста C для восстановления открытого текста P.

Из этих двух формул следует, что $D_K(E_K(P)) = P$.

Такая нотация предполагает, что E и D являются просто *математическими функциями*.

Основы криптографии

Правила и принципы

Основное правило криптографии состоит в предположении, что криптоаналитику (взломщику кода) известен используемый метод шифрования - злоумышленник точно знает, как работает метод шифрования ***E***.

Принцип Керкгофа (1883) гласит:
Алгоритмы шифрования общедоступны; секретны только ключи.

Чем длиннее ключ, тем выше показатель трудозатрат взломщика кода. При увеличении длины ключа показатель трудозатрат для взлома системы путем простого перебора значений ключа растет экспоненциально.

Основы криптографии

Метод подстановки

Каждый символ или группа символов заменяется другим символом или группой символов:

- **Шифр Цезаря** - заменяет все буквы алфавита на другие с помощью циклического сдвига на три позиции.
- **Моноалфавитная подстановка** - ключом является 26-символьная строка, соответствующая полному алфавиту:

abcdefghijklmnopqrstuvwxyz

qwertyuiopasdfghjklzxcvbnm

$26! = 4 \times 10^{26} \times 1нс = 10^{10}$ лет

Основы криптографии

Метод подстановки (взлом)

Используются статистические характеристики естественных языков.

В английском языке:

буква *e* встречается в тексте **чаще всего**, за ней по частоте использования идут буквы *t, o, a, n, i* и т. д.

наиболее часто встречающимися комбинациями из двух символов (**биграммами**) являются *th,in, er, re* и *an*.

наиболее часто встречающимися комбинациями из трех символов (**триграммами**) являются *the, ing, and* и *ion*.

Основы криптографии

Метод перестановки

Меняют порядок следования символов, но не изменяют сами символы.

m	e	g	a	b	u	c	k
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Открытый текст
pleasetransferonemilliondollar
stomyswissbankaccountsixtwo
two

Зашифрованный текст
afllsksoselawaiatoossctclnmo
mantesilyntwrnntsowdpaedobu
oeriricxb

Please transfer one million dollars to my swiss bank account six two two

Основы криптографии

Метод перестановки (взлом)

Вначале надо понять, что **шрифт перестановочный**. Это легко заметить по частоте символов *e, t, o, a, n, i* и. т.д.

Затем нужно угадать **число колонок**. Для каждой длины ключа в шифрованном тексте образуется различный набор биграмм. Перебрав различные варианты, часто довольно легко может определить длину ключа.

Остается узнать только **порядок колонок**.

Если число колонок *k* невелико, можно перебрать все *k*(*k* - 1) возможных комбинаций пар соседних колонок, сравнивая частоты образующихся биграмм со статистическими характеристиками английского языка. Пара с лучшим соответствием считается правильно позиционирванной. Затем все оставшиеся колонки по очереди проверяются в сочетании с уже найденной парой. Колонка, в которой биграммы и триграммы дают максимальное совпадение со статистикой, предполагается правильной. Есть шанс, что на данном этапе текст уже будет распознаваемым (например, если вместо слова *million* мы увидим *milloin,* то сразу станет ясно, где сделана ошибка).

Основы криптографии

Одноразовые блокноты

В зашифрованном сообщении не содержится **никакой информации** для взломщика, поскольку любое открытое сообщение является равновероятным кандидатом.

I love you.

Открытое сообщение 1

I		I	o	v	e		y	o	u	.
49	20	6C	6F	76	65	20	79	6F	79	2E
1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110

Последовательность 1 (одноразовый блокнот 1)

1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011

Зашифрованный текст: ***ОС1 + П1***

0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Последовательность 2 (одноразовый блокнот - случайный)

1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110

Открытое сообщение 2

1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

E	l	v	l	s		l	l	v	e	s

Elvis lives

Основы криптографии

Квантовая криптография

Протокол **BB84** - (Bennet и Brassard, 1984).

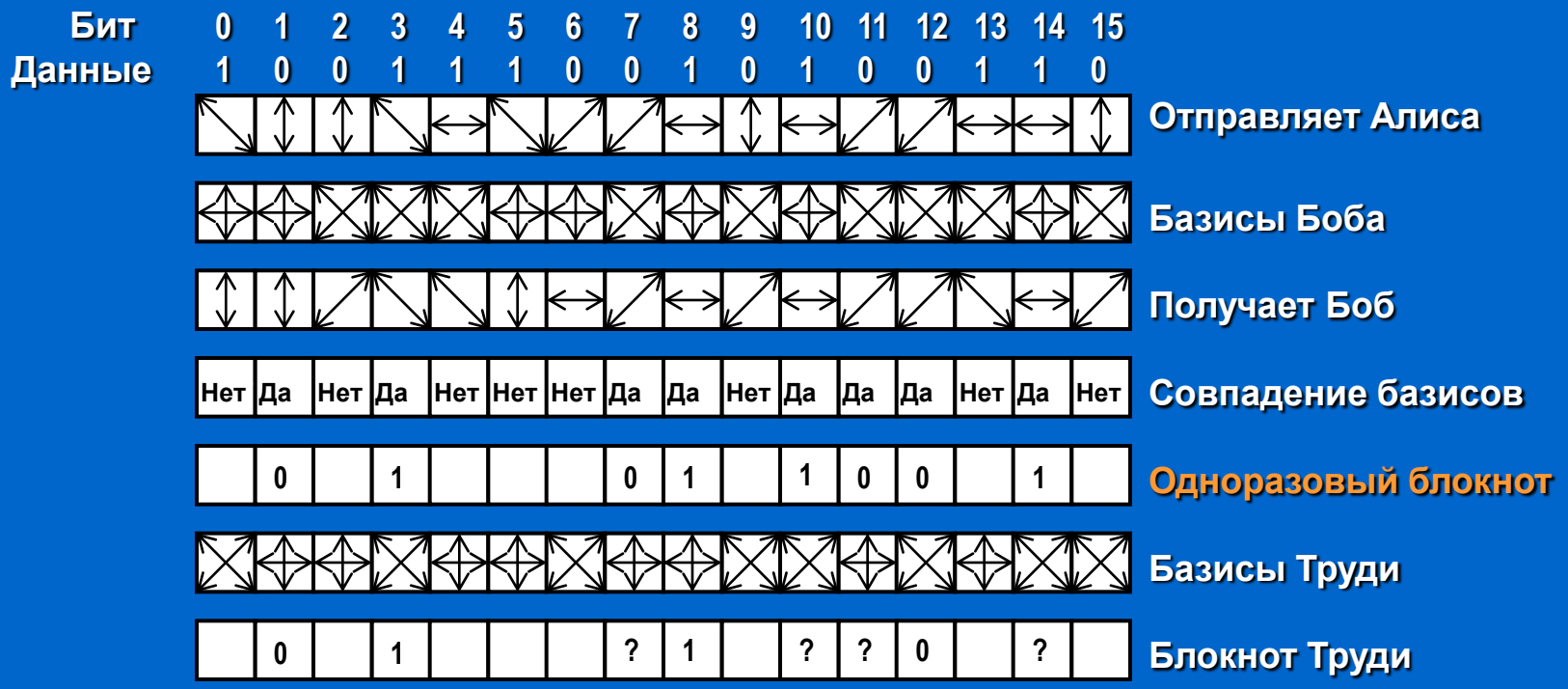
Принципиалы - **Алиса** передает по кабелю одноразовую последовательность **Бобу**.

Шпион – **Труди** установила на пути кабеля активное подслушивающее устройство. Она может считывать сигналы, идущие в обоих направлениях. Кроме того, она может посылать как в одну, так и в другую сторону фальшивые сообщения.

Основы криптографии

Квантовая криптография

Прямолинейный (↕ - 1, ↔ - 0) и ***диагональный*** (↘ - 1, ↗ - 0) базис.



На основе одноразового блокнота возможно усиление секретности.

Основы криптографии

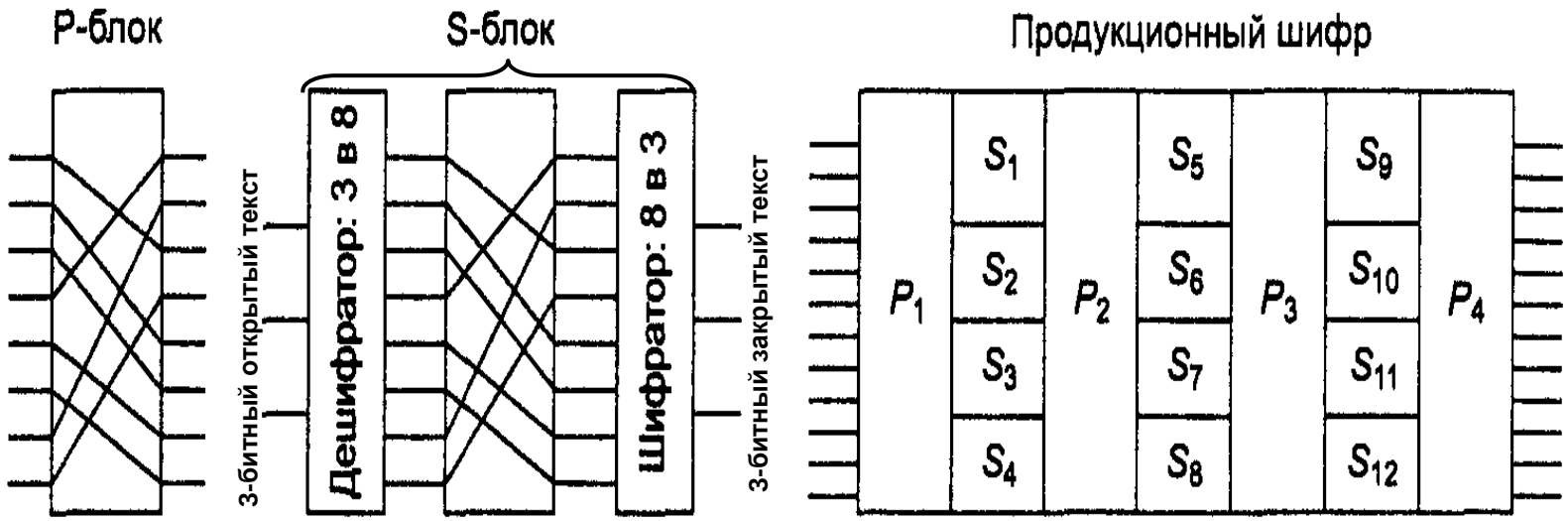
Два фундаментальных принципа

1: Сообщения должны содержать избыточные данные.

2: Необходим способ борьбы с повторной отправкой посланных ранее сообщений.

Алгоритмы с симметричным ключом

Продукционный шифр

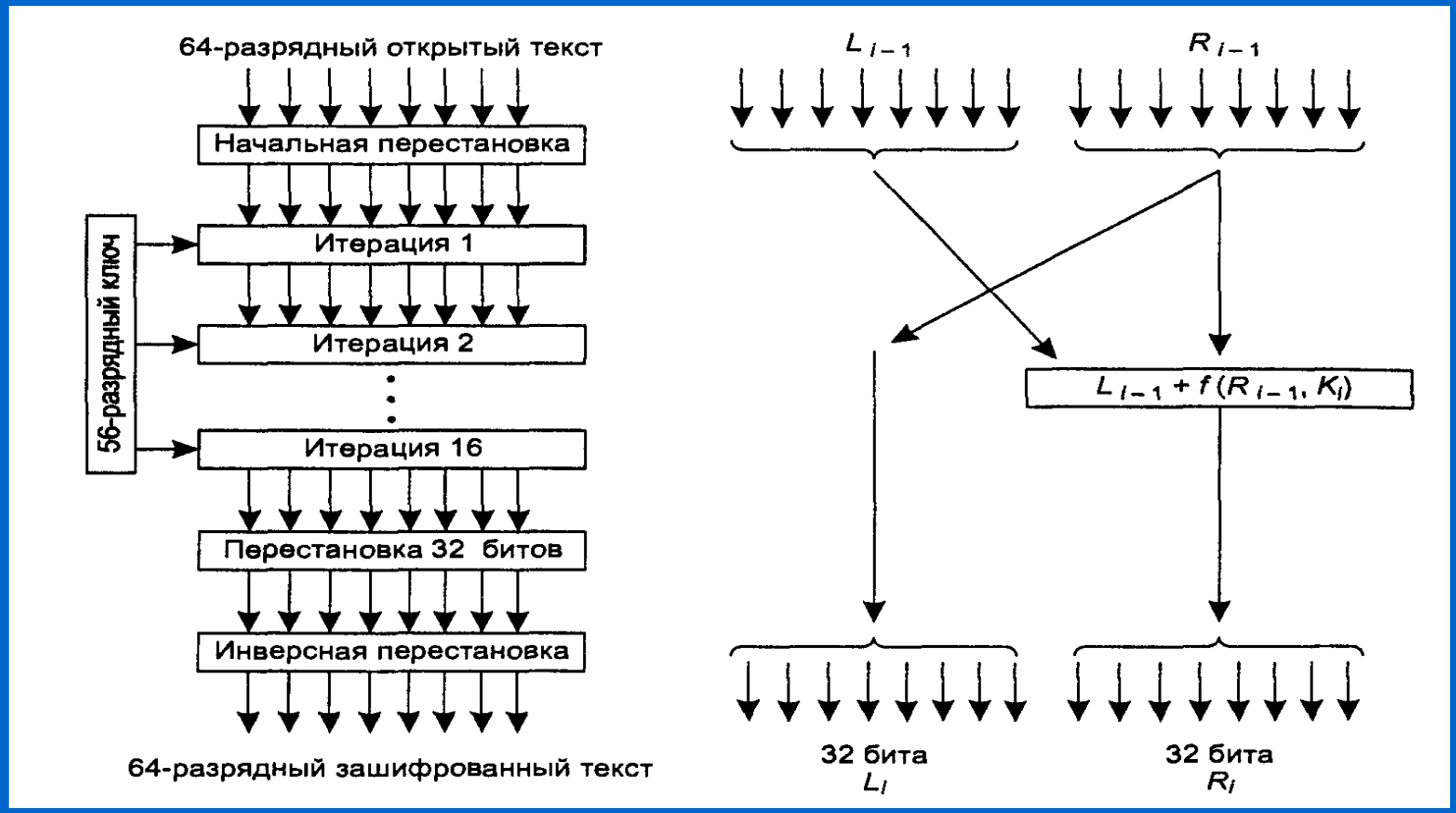


P – *permitation* – перестановка, S – *substitution* – подстановка, замена

Продукционные шифры, работающие с k-битными входами и производящие k-битные последовательности, широко распространены. Обычно значение *k* колеблется от 64 до 256.

Алгоритмы с симметричным ключом

Стандарт шифрования данных (DES)



Стандарт DES (**Data Encryption Standard** — стандарт шифрования данных), **разработанный фирмой IBM, принят правительством США в январе 1977 году в качестве официального стандарта.**

Алгоритмы с симметричным ключом

Стандарт шифрования данных (DES)

Правительство США пригласило **IBM** на обсуждение этого вопроса с Агентством национальной безопасности, **NSA (National Security Agency)**, являющимся самым крупным в мире работодателем в области математики и криптоанализа. Агентство национальной безопасности США настолько секретно, что существует даже такая популярная шутка:

Вопрос: ***Что означает аббревиатура NSA?***
Ответ: ***No Such Agency — такого агентства нет.***

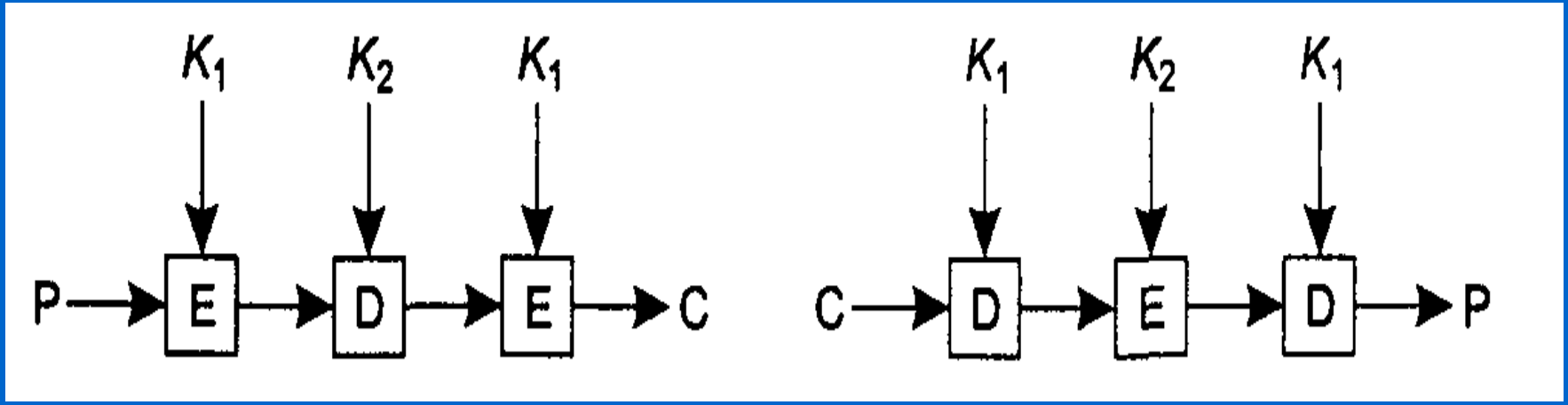
После этих обсуждений корпорация IBM уменьшила длину ключа со 128 до 56 бит и решила держать в секрете процедуру разработки стандарта DES. Многие полагали, что длина ключа была уменьшена, чтобы гарантировать, что NSA сможет взломать DES, но организациям с более низким финансированием это будет не по силам.

В 1977 году ученые Стэнфордского университета **Диффи (Diffie) и Хеллман (Hellman)**, разработали машину для взлома кода DES и оценили стоимость ее создания в 20 млн долларов.

Алгоритмы с симметричным ключом

Тройное шифрование с помощью DES

Международный стандарт 8732 (с 1979 года).



Почему EDE, а не EEE ?

Почему K1, K2 ?

Алгоритмы с симметричным ключом

Улучшенный стандарт шифрования AES

В январе 1997 года ученые со всего мира были приглашены для представления своих разработок, касающихся нового стандарта, который назвали **AES** (**Advanced Encryption Standard** — улучшенный стандарт шифрования).

Требования, предъявляемые к разработкам, были таковы:

1. Алгоритм должен использовать симметричный блочный шифр.
2. Все детали разработки должны быть общедоступны.
3. Должны поддерживаться длины ключей 128, 192 и 256 бит.
4. Должна быть возможна как программная, так и аппаратная реализация.
5. Алгоритм должен быть общедоступным или базирующимся на не дискредитировавших себя понятиях.

Было рассмотрено 15 серьезных предложений.

Алгоритмы с симметричным ключом

Улучшенный стандарт шифрования AES

В августе 1998 года Институтом стандартов и технологий были выбраны пятеро финалистов. Выбор основывался в основном на таких аспектах, как обеспечиваемая безопасность, эффективность, простота, гибкость, а также требования к памяти (это важно для встроенных систем). Результаты выглядели следующим образом:

1. **Rijndael** (Qohn Daemen, Vincent Rijmen), 86 голосов.
2. **Serpent** (Ross Anderson, Eli Biham, Lars Knudsen), 59 голосов.
3. **Twofish** (команда, возглавляемая Bruce Schneier), 31 голос.
4. **RC6** (компания RSA Laboratories), 23 голоса.
5. **MARS** (корпорация IBM), 13 голосов.

В октябре 2000 года NIST (Национальный институт стандартов и технологий) объявил о том, что он также голосует за **Rijndael**, и уже в ноябре 2001 года **Rijndael** становится стандартом правительства США, опубликованным как **Федеральный стандарт обработки информации, FIPS 197.**

Улучшенный стандарт шифрования AES

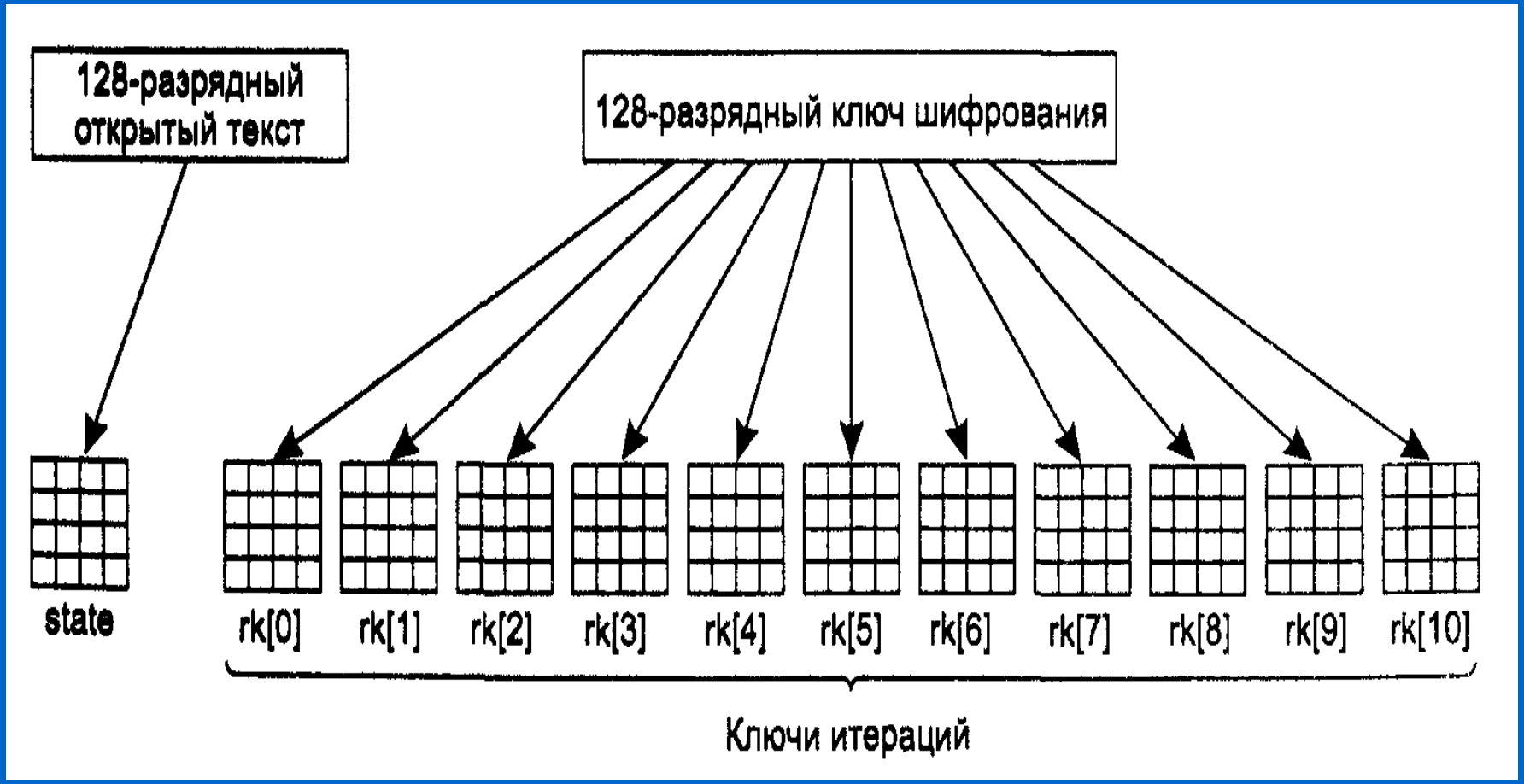
Алгоритм метода Rijndael

```
#define LENGTH 16/* Число байтов в блоке данных или ключе */
#define NROWS 4/* Число строк в массиве state */
#define NCOLS 4/* Число столбцов в массиве state */
#define ROUNDS 10/* Число итераций */
typedef unsigned char byte/8-разрядное целое без знака */

rijndael(byte plaintext[LENGTH], byte ciphertext[LENGTH], byte key[LENGTH])
{
int r;/* Счетчик цикла */
byte state[NROWS][NCOLS];/* Текущее состояние */
struct{byte k[NROWS][NCOLS];} rk[ROUNDS + 1];/* Ключи итерации */

expand_key(key,rk);/* Сформировать ключи итерации */
copy_plaintext_to_text(state, plaintext);/* Инициализация текущего состояния */
xor_roundkey_into_state(state, rk[0]);/* Сложить по модулю 2 ключ с текущим состоянием
*/

for(r=1; r<=ROUNDS; r++) {
substitute(state);/* Пропустить каждый байт через S-блок */
rotate_rows(state);/* Повернуть строку i на i байт */
if(r < ROUNDS) mix_columns(state);/* Смешивающая функция */
xor_roundkey_into_state(state, rk[r]);/* Сложить по модулю 2 ключ с текущим состоянием
*/
}
copy_state_to_ciphertext(ciphertext, state);/* Вернуть результат */
}
```

plaintext — массив размером 16 байт, содержащий входные данные, **ciphertext** — массив размером 16 байт, в который будет возвращен шифр, а также key — 16-разрядный ключ. В процессе вычислений текущее состояние данных сохраняется в байтовом массиве state, размер которого равен NROWS x NCOLS. Для 128-битных блоков данных размер этого массива равен 4x4 байта. В 16 байтах целиком уместится один блок.

Улучшенный стандарт шифрования AES

Схематичный алгоритм метода Rijndael



Программная реализация на машине с частотой **2 ГГц** может шифровать данные со скоростью **700 Мбит/с**. Аппаратные реализации работают еще быстрее.