



Модели организации сетей

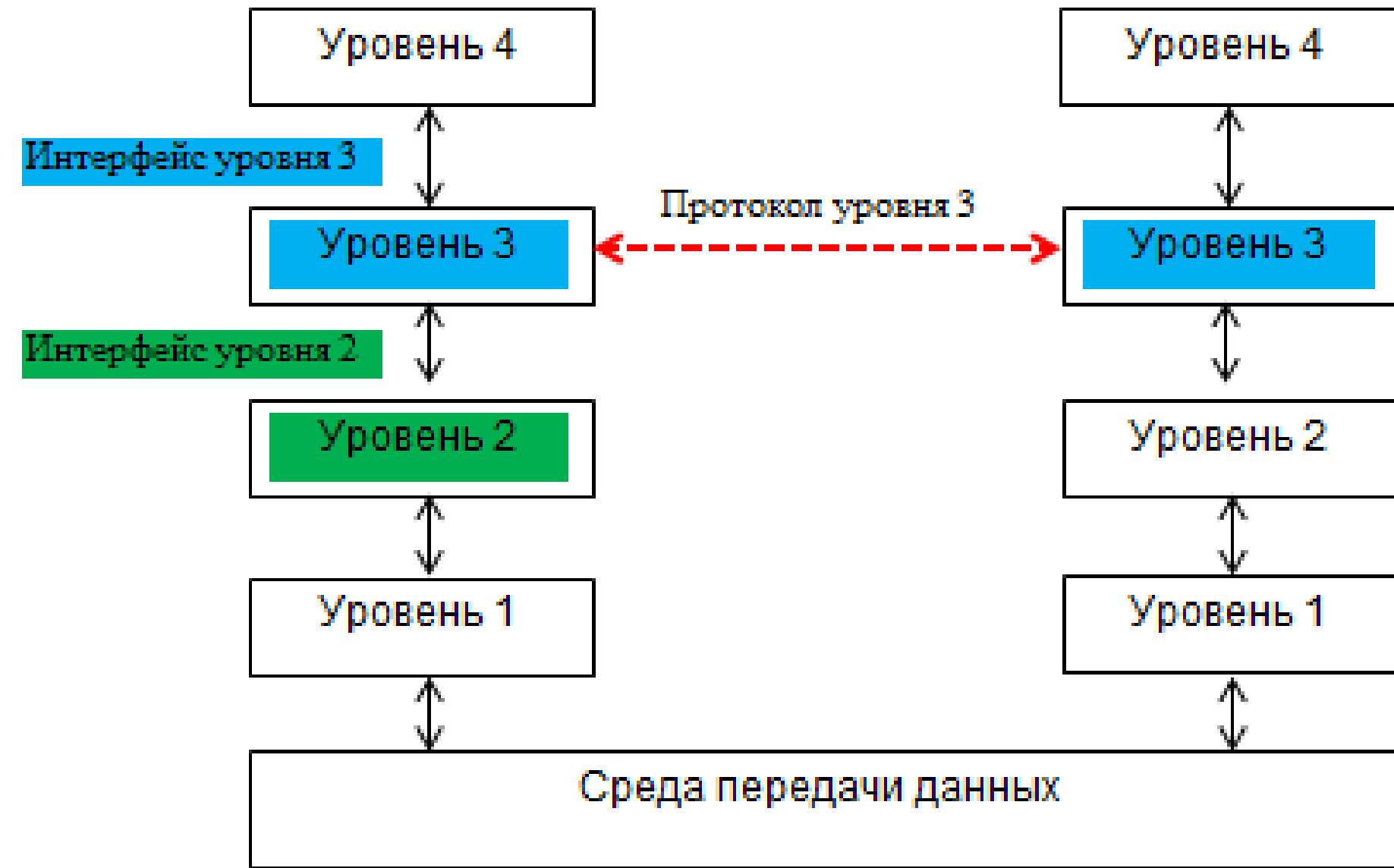


Сложности построения сетей

- разное оборудование, ПО
- надежность
- развитие сети
- распределение ресурсов
- безопасность

Решение: декомпозиция на подзадачи (уровни)

- уровень решает конкретную задачу или несколько связанных задач
- уровни изолированы - если в сети произошли изменения, не нужно менять всё ПО или оборудование, а только то, которое относится к уровню, на котором произошли изменения



Сервис - описывает что полезное делает уровень.

Интерфейс - набор операций, которые нижний уровень предоставляет верхнему (реальное общение внутри одного компьютера).

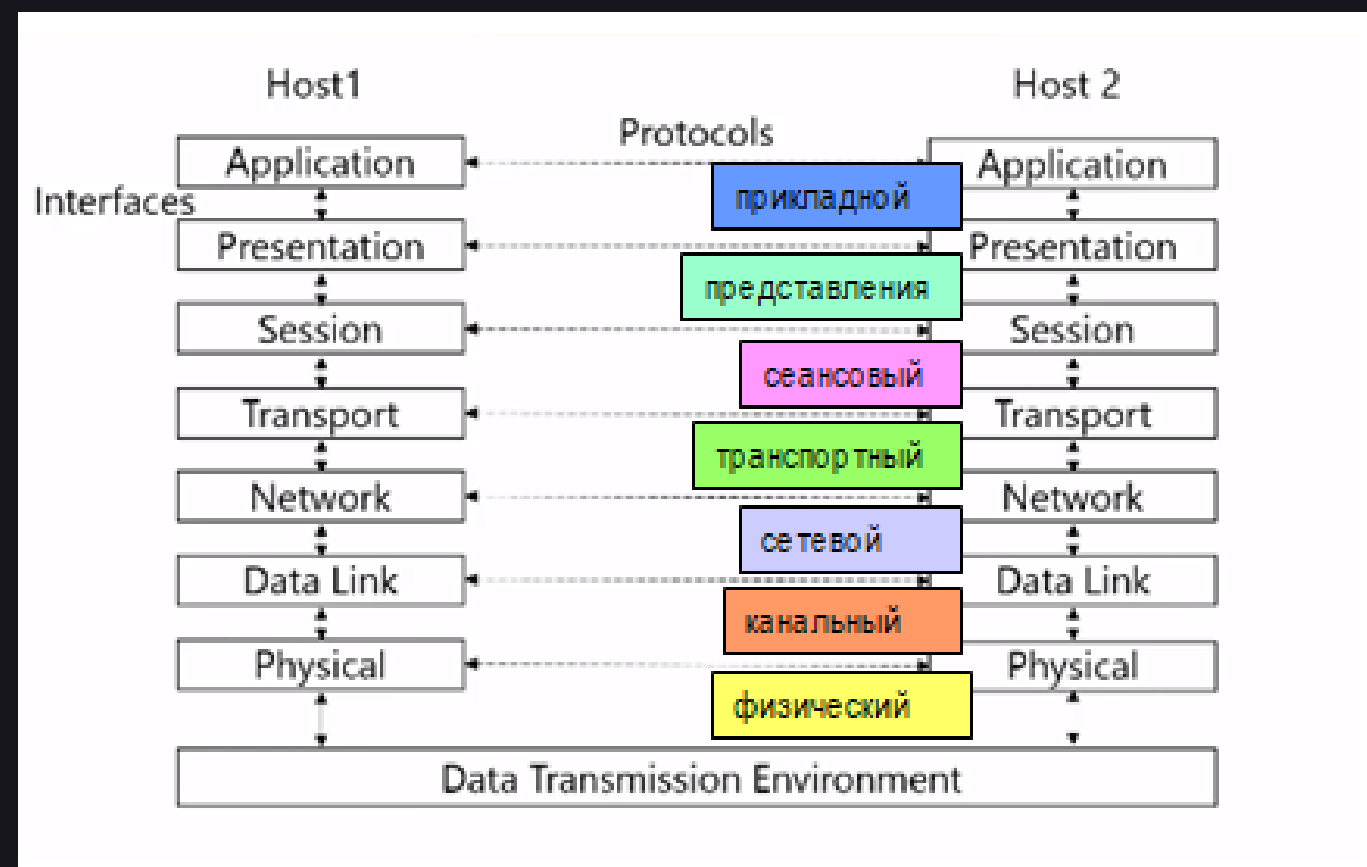
Протокол - правила и соглашения, которые используются для связи разных хостов на одном уровне (виртуальное общение между компьютерами).

сколько уровней должно
 быть?
какие уровни должны
 быть?
какие функции должны
 выполняться на каждом
 уровне ?

Архитектура

Набор уровней и протоколов сети
(интерфейсы не входят)

Модель OSI



OSI Модель взаимодействия открытых систем

- Юридический стандарт международной организации стандартизации ISO
- 7 уровней, протоколы не входят в модель
- хорошая теоретическая проработка
- не используется на практике

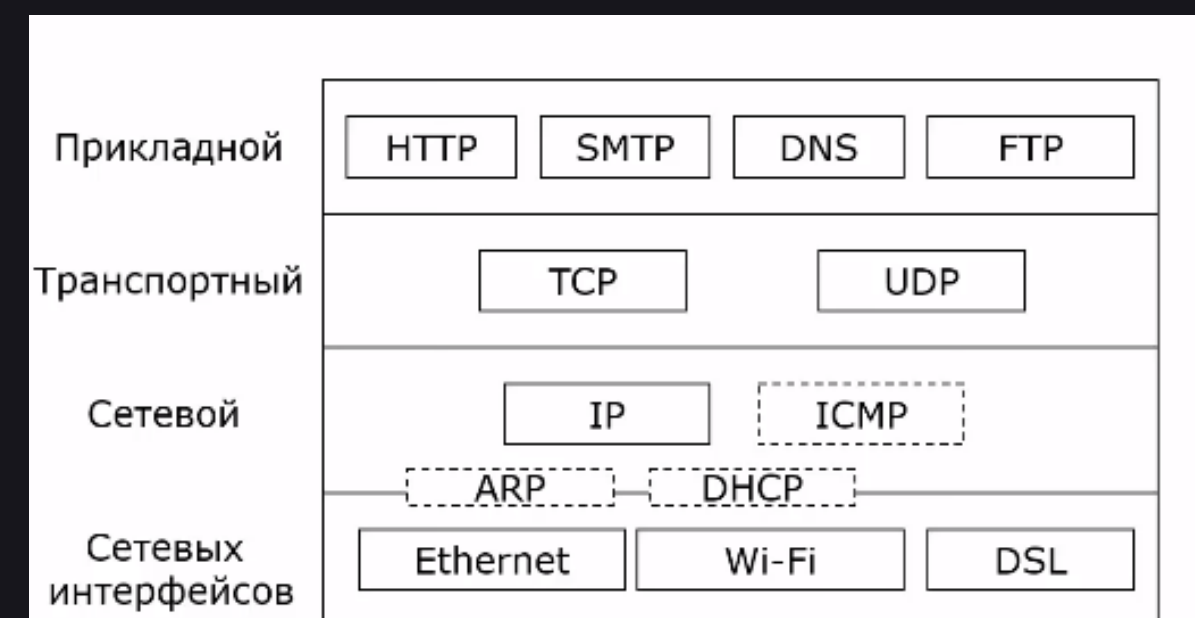
TCP/IP

- Фактический стандарт на основе стека TCP/IP
- 4 уровня
- протоколы широко используются на практике

OSI vs TCP/IP

Модель OSI	Модель TCP/IP
Прикладной	Прикладной
Представления	
Сеансовый	
Транспортный	Транспортный
Сетевой	Интернет
Канальный	Сетевых интерфейсов
Физический	

Стек протоколов TCP/IP



Физический уровень

Сервис - передача потока бит по среде передачи данных

1

Физический уровень представляет информацию в виде сигналов

Среда передачи данных:

- телефонный кабель
- **оптический кабель**
- витая пара
- радиоволны

Ошибки
очень редко
редко
часто

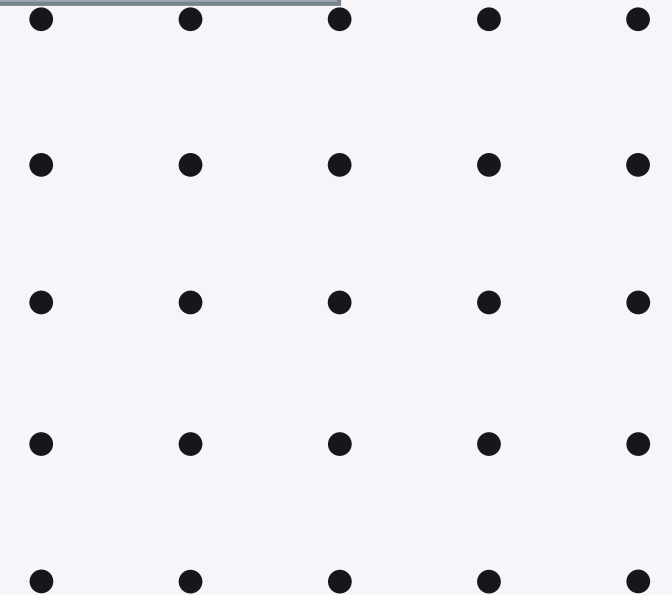
2

несколько источников сигнала искажают друг друга

для разных технологий выделяют разные диапазоны

- сотовая связь - 900 МГц
- Wi-Fi - 2,4 ГГц и 5 ГГц

Единица
передачи
информации
Бит



Канальный уровень

Единица передачи информации

**Кадр
(Frame)**

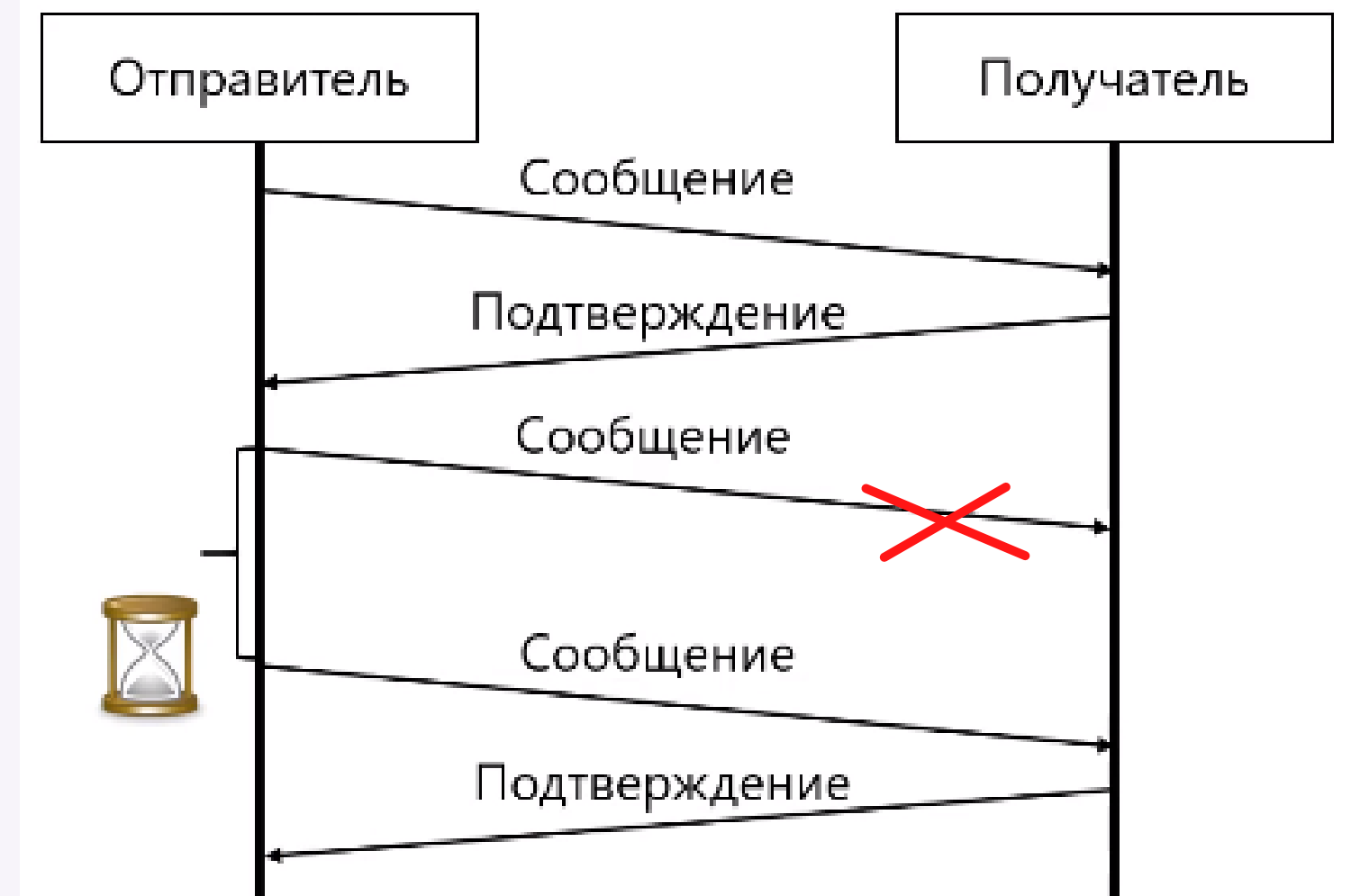
1

- Задача - передача **сообщений** по каналам связи
- определение начала и конца сообщения в потоке бит
 - исправление ошибок
 - адресация
 - согласованный доступ к каналу

2

- Исправление ошибок
- повторная отправка сообщения (метод "остановка и ожидание")
 - обнаружение и исправление

Повторная отправка сообщения



Канальный уровень имеет **2** подуровня



Подуровень управления логическим каналом

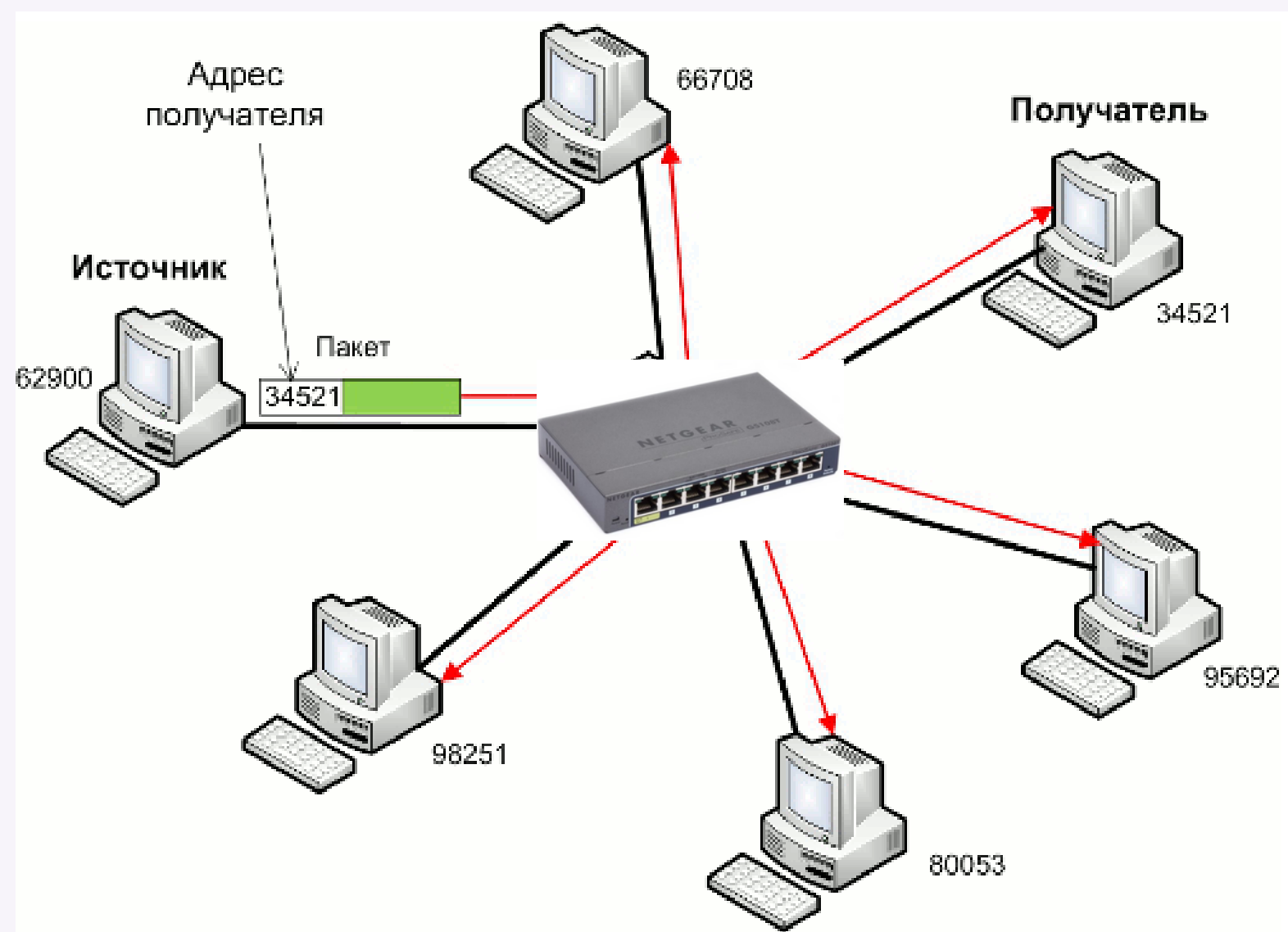
Отвечает за передачу данных (создание кадров, обработка ошибок)



Подуровень управления доступом к среде

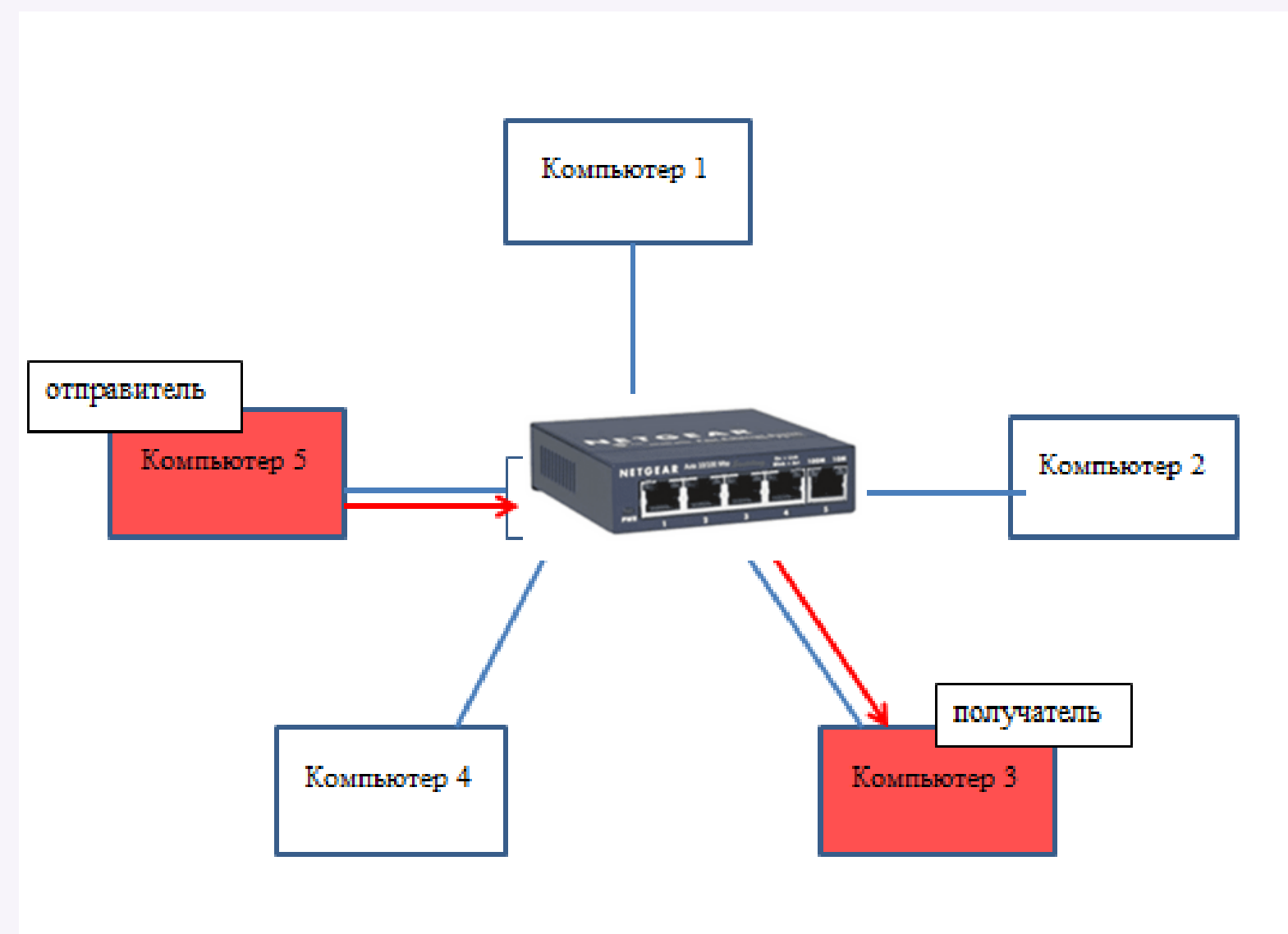
- Совместное использование разделяемой среды (может возникнуть "**Коллизия**", если несколько компьютеров начнут передачу одновременно)
- Адресация

Концентратор



Физический уровень

Коммутатор



Канальный уровень

MAC адрес

Физический адрес : C0-38-96-62-4A-C7

С его помощью мы понимаем кому адресованы данные, если у нас на канале связи несколько устройств.

2

Длина MAC-адреса 6 байт
Форма записи - 6 шестнадцатеричных чисел
ipconfig /all (Windows)
ip address (Linux)

3

Назначается централизованно - производителем оборудования
либо
Локально - администратором

Индивидуальный unicast
30-9C-23-15-E8-8C

Групповой multicast
01-80-C2-00-00-08

Широковещательный broadcast
FF-FF-FF-FF-FF-FF

Ethernet

Сетевая технология для
проводной связи

Классический
1973

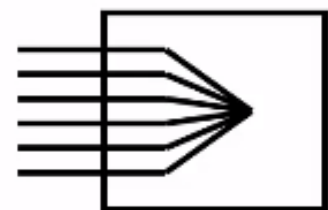
Разделяемая среда
устройство -
Концентратор Hub

Плохая
масштабируемость
(снижается скорость)
Низкая безопасность
(данные доступны всем)

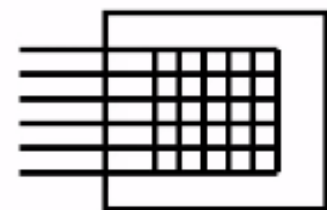
Коммутируемый
1995

Точка-точка
Нет разделяемой среды
нет коллизий
устройство - Коммутатор
Switch
все порты связаны друг
с другом напрямую
Таблица коммутации

Концентратор (hub)



Коммутатор (switch)



Wi-Fi

Технология беспроводных
локальных сетей

Адресация через MAC-адреса
Разделяемая среда - радиоэфир
Формат кадра на уровне LLC одинаковый

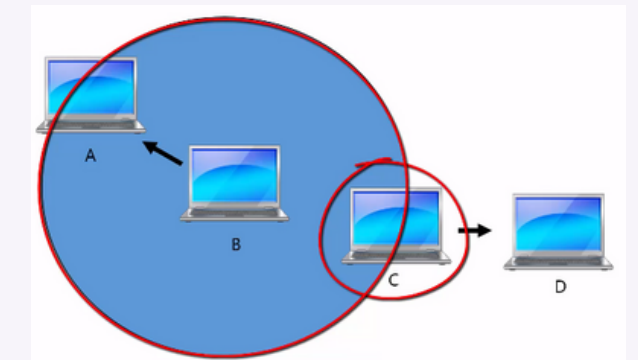
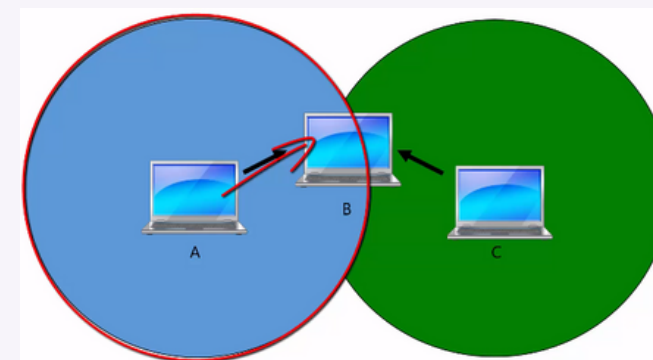
Особенности среды

- вероятность ошибки передачи гораздо выше
- мощность передаваемого сигнала выше принимаемого
- не все компьютеры в сети получают данные - проблемы скрытой и засвеченной станции

Из-за большого количества ошибок используется

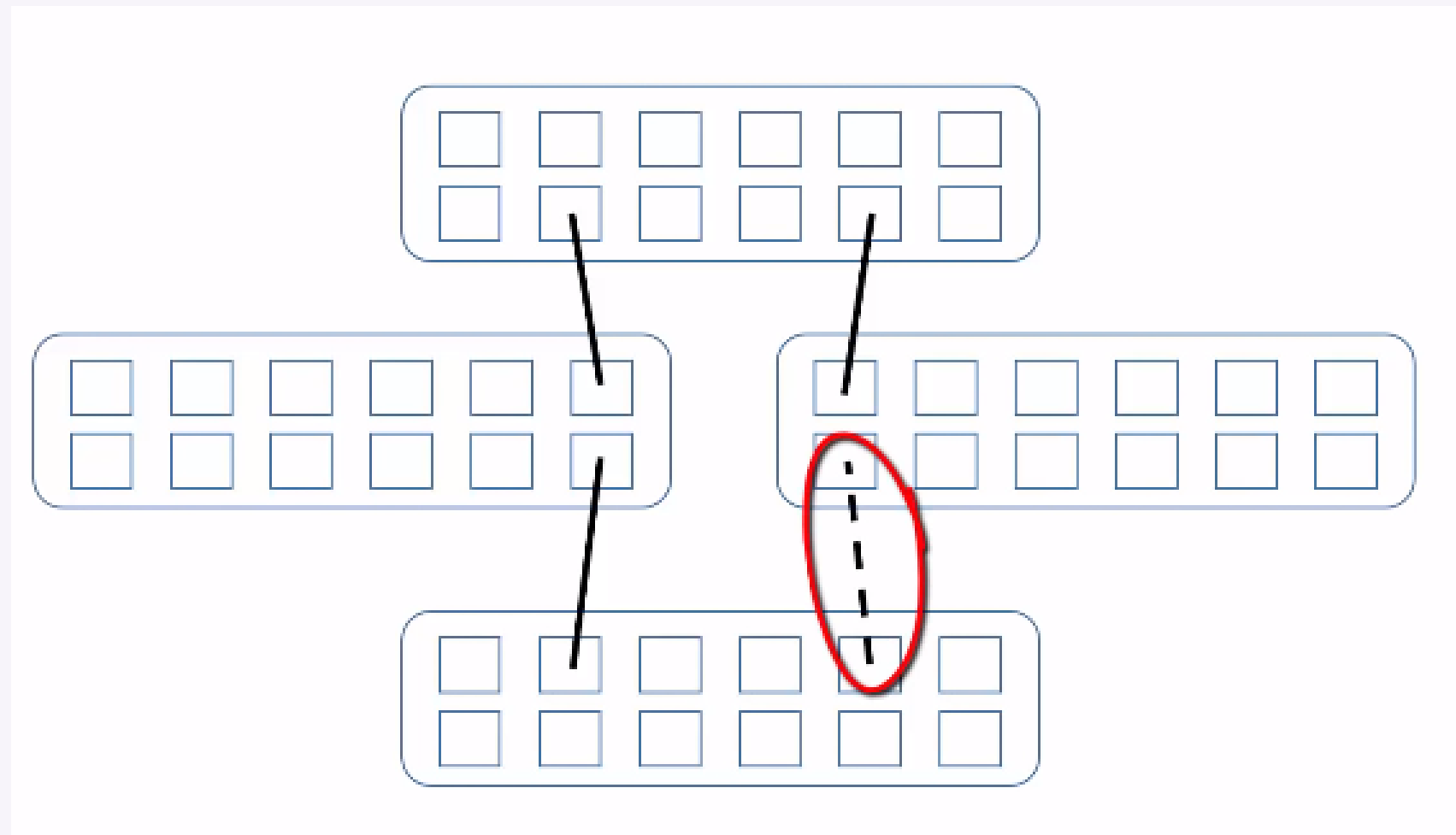
подтверждение получения данных

Коллизии обнаруживаются по отсутствию подтверждения, в Wi-Fi коллизии очень дорогие



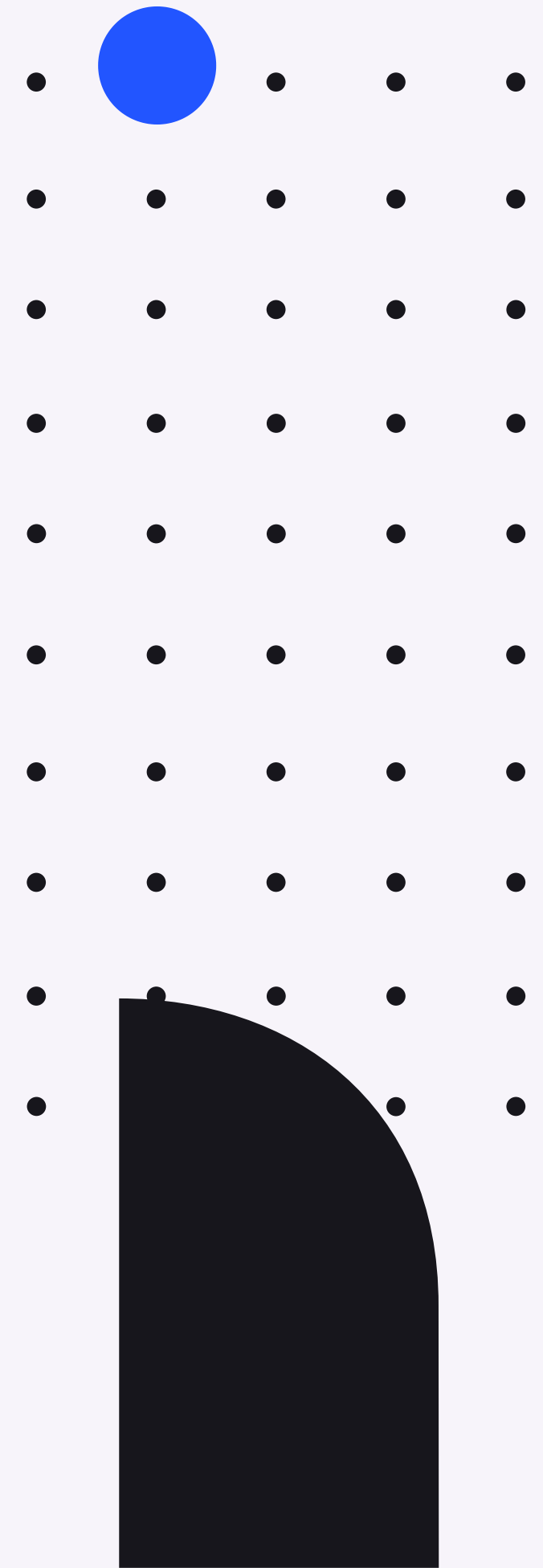
Протокол STP

Spanning Tree Protocol (протокол связующего дерева)



Автоматическое отключение дублирующих путей в Ethernet. Решается проблема **широковещательного шторма**.

Сейчас используется RSTP - он быстрее, принцип тот же.



Сетевой уровень



Построение крупной сети из отдельных сетей, которые построены на разных технологиях (Ethernet, Wi-Fi, 5G, 4G, 3G)
Сети могут отличаться сервисами, возможностью поддерживать широковещание, максимальным размером кадра и др



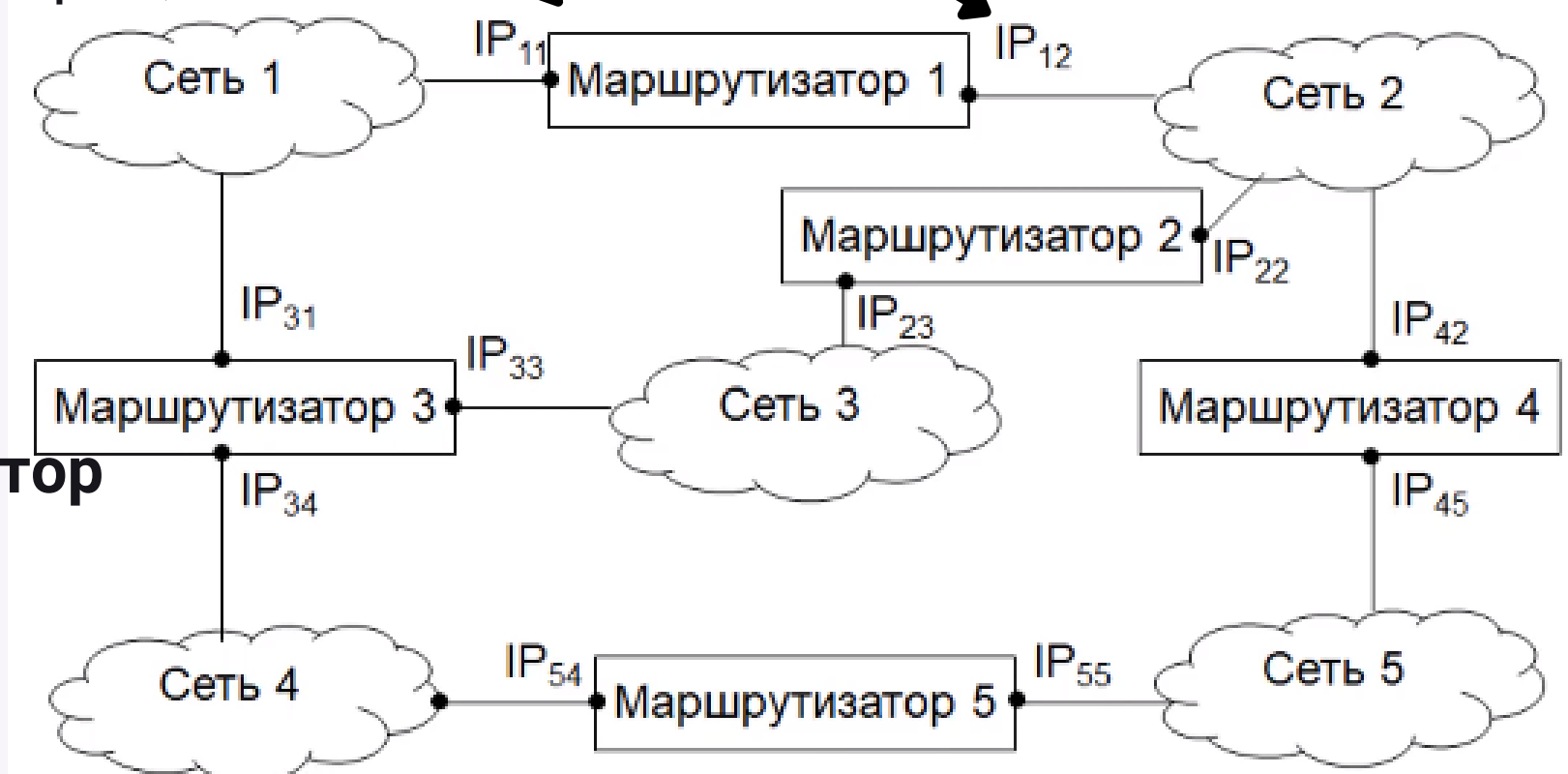
Глобальные адреса - IP адреса
Фрагментация (сети могут быть разных размеров, размер данных > размера сети)



Основные задачи уровня
- объединение сетей
- маршрутизация - используется **маршрутизатор**
разные пути к сети

Данные передаются пакетами

Есть несколько интерфейсов
у каждого интерфейса свой IP-адрес



IP-адреса



Две версии протокола IP

- IPv4 - адрес 4 байта
- IPv6 - адрес 16 байт



IPv4 - 4 десятичных числа от 0 до 255 разделенных точкой

213.180.193.3

На сетевом уровне идет работа не с отдельными адресами, а с подсетями (старшая часть IP-адреса одинаковая)



IP-адрес 213.180.193.3 ← адрес хоста
адрес подсети

- 213.180.193.1
- 213.180.193.2
- 213.180.193.3
- ...
- 213.180.193.254

Виды IP-адресов

- Индивидуальный
- Групповой
- Широковещательный 213.180.193.255
- Статические
- Динамические
- Внешние
- Внутренние

Маска подсети

Десятичное представление:

- IP-адрес: 213.180.193.3
- Маска подсети: 255.255.255.0
- Адрес подсети: 213.180.193.0

В виде префикса:

- 213.180.193.3 /24
- Адрес подсети: 213.180.193.0

Протокол IP



Протокол межсетевого взаимодействия (для передачи данных)

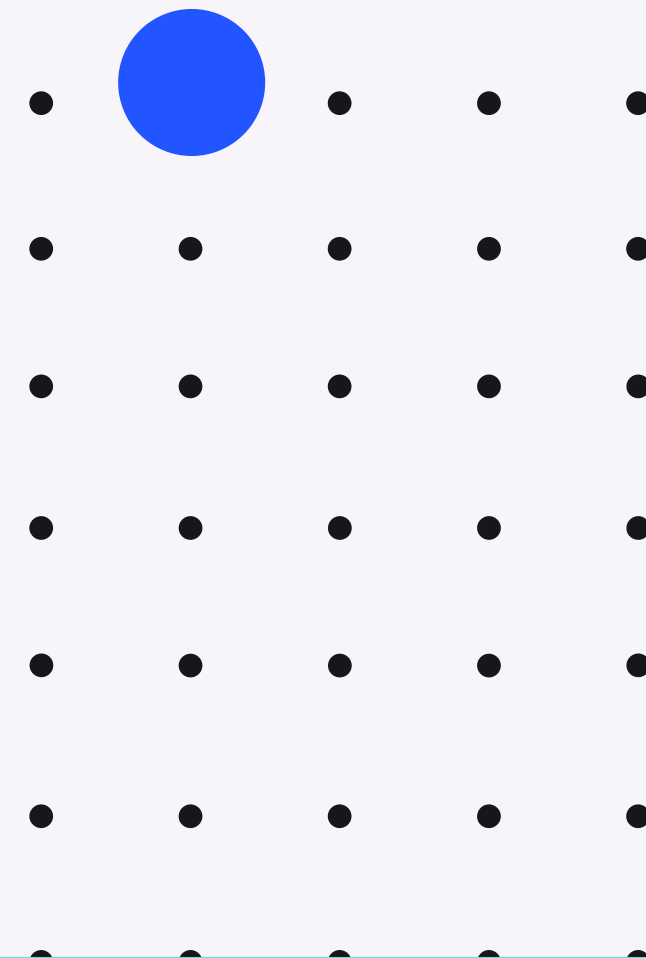
- без гарантии доставки
- без сохранения порядка следования сообщений
- БЕЗ УСТАНОВКИ СОЕДИНЕНИЯ

если пакет не дошел, ничего не происходит
ошибка должна быть устранена на вышестоящих уровнях



Задачи протокола

- маршрутизация
- объединение сетей



Записи в таблице маршрутизации

Статические

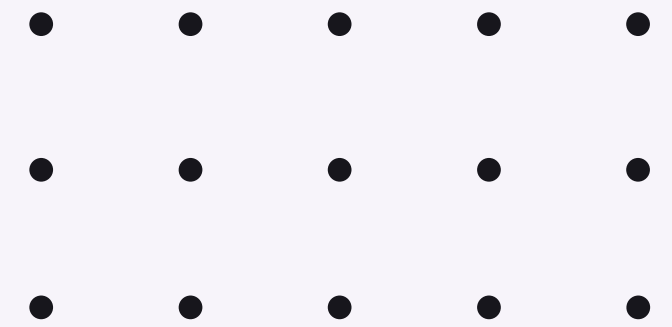
- Настраиваются вручную
- Конфигурация интерфейсов
- Вручную прописанные маршруты к сетям

Динамические

- Настраиваются автоматически
- Протоколы маршрутизации RIP, OSPF, BGP и др.

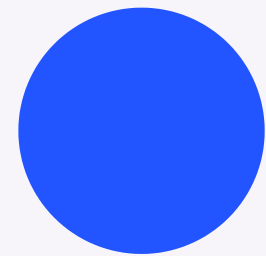
DHCP

Dynamic Host Configuration Protocol

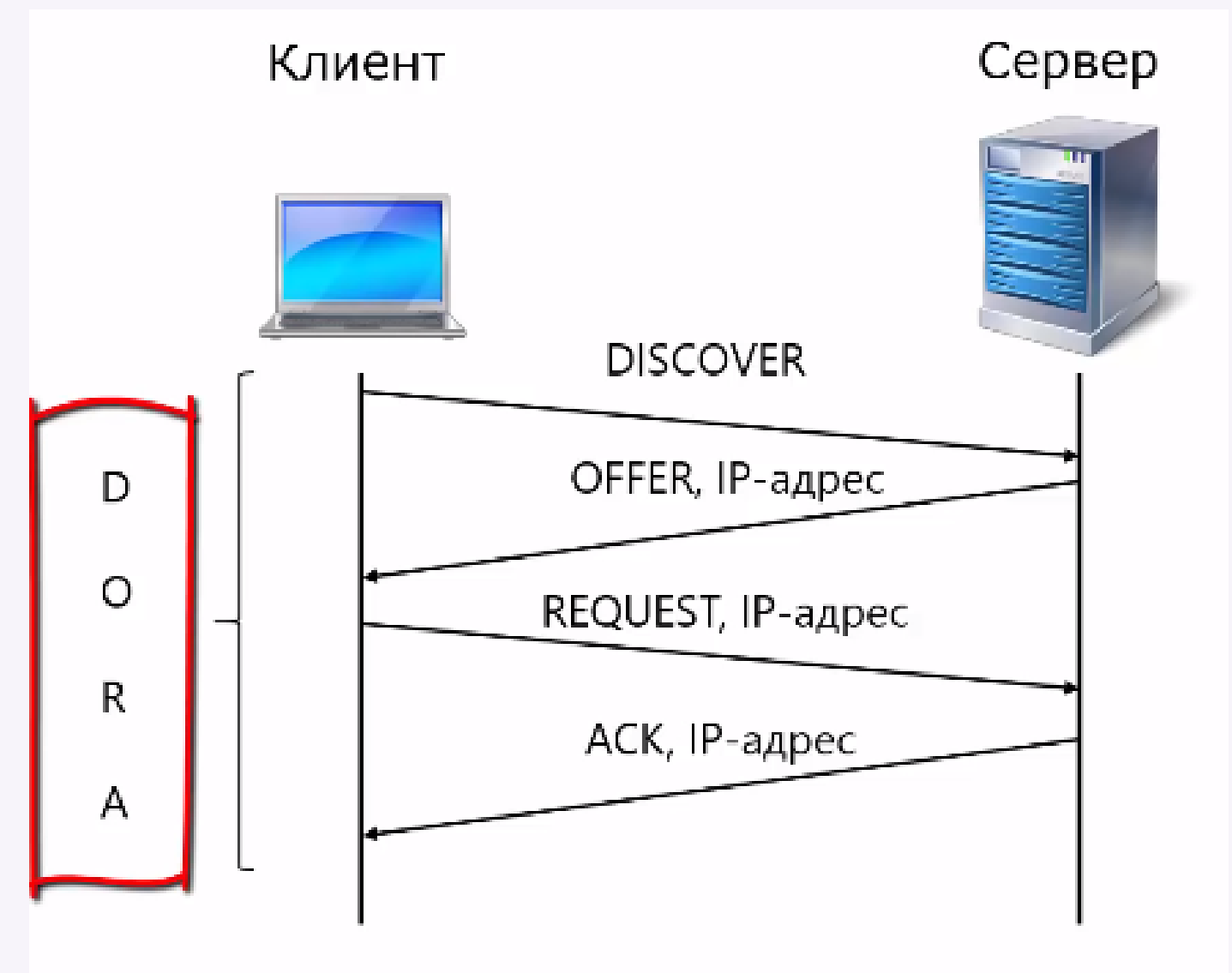


Протокол динамической конфигурации хостов - позволяет назначать IP-адреса для компьютеров в сети автоматически

- IP-адреса компьютеров могут меняться
- DHCP работает по модели клиент-сервер (необходим DHCP сервер)



IP-адрес выдается на ограниченное время
Клиент может продлить аренду, это происходит после истечения половины времени, делает новый запрос на сервер и просит продлить



ARP (Address Resolution Protocol)



Протокол разрешения адресов -
позволяет по IP-адресу компьютера определить
MAC-адрес

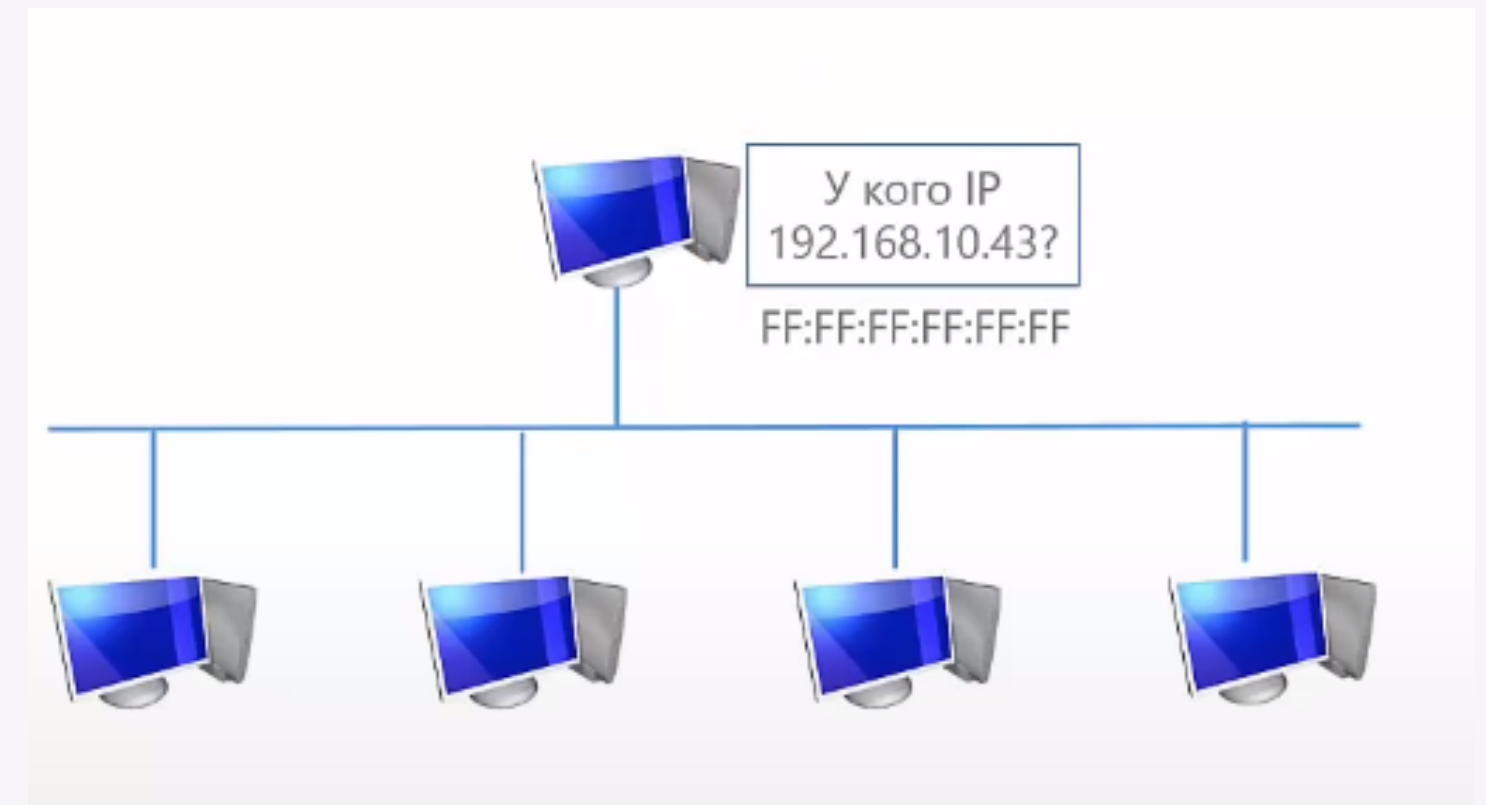
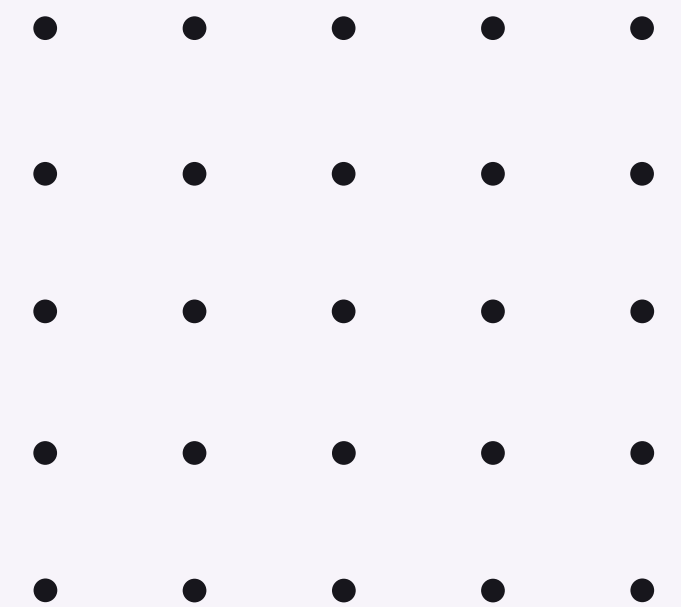


Запрос посылается на широковещательный
адрес
Ответ присылает только компьютер с
соответствующим IP



ARP не проходит через маршрутизатор

После обнаружения MAC-адрес кешируется в
ARP таблице



ICMP (Internet Control Message Protocol)

Протокол межсетевых управляющих сообщений

Функции:

- Оповещение об ошибках на сетевом уровне

- Тестирование работоспособности сети

сообщения об ошибках не обязательно должны обрабатываться

Большая часть пакетов ICMP формируются и отправляются сетевым оборудованием автоматически. Некоторые сообщения формируются утилитами. Утилиты применяются для диагностики сети:

ping -проверяет доступность компа в сети

```
C:\Users\alena>ping google.by

Обмен пакетами с google.by [172.217.16.4] с 32 байтами данных:
Ответ от 172.217.16.4: число байт=32 время=56мс TTL=115
Ответ от 172.217.16.4: число байт=32 время=55мс TTL=115
Ответ от 172.217.16.4: число байт=32 время=54мс TTL=115
Ответ от 172.217.16.4: число байт=32 время=55мс TTL=115

Статистика Ping для 172.217.16.4:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 54мсек, Максимальное = 56 мсек, Среднее = 55 мсек
```

tracert - находит адреса всех маршрутизаторов, через которые проходит пакет

```
C:\Users\alena>tracert tut.by

Трассировка маршрута к tut.by [178.172.160.5]
с максимальным числом прыжков 30:

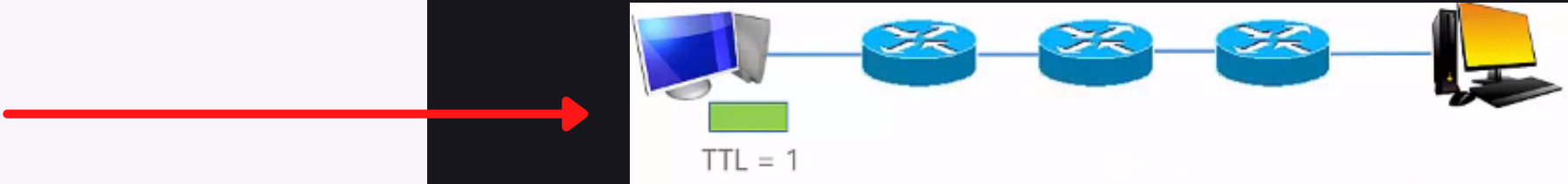
 1  <1 мс    <1 мс    <1 мс    192.168.0.1
 2   2 мс     2 мс     2 мс     192.168.1.1
 3  25 мс    25 мс    26 мс    100.64.0.1
 4  26 мс    25 мс    28 мс    grodnoreg.10g.net.belpak.by [93.85.240.220]
 5  28 мс    24 мс    29 мс    10.0.42.53
 6  33 мс    33 мс    33 мс    core1.net.belpak.by [93.85.253.69]
 7  29 мс    30 мс    30 мс    93.84.125.189
 8  30 мс    30 мс    30 мс    178.124.134.165
 9  30 мс    28 мс    29 мс    178-172-160-5.hosterby.com [178.172.160.5]

Трассировка завершена.
```

Пакет ICMP включает тип сообщения и код сообщения

Тип	Назначение сообщения
0	Эхо-ответ
3	Узел назначения недостижим
5	Перенаправления маршрута
8	Эхо-запрос
9	Сообщение о маршрутизаторе
10	Запрос сообщения о маршрутизаторе
11	Истечение времени жизни пакета
12	Проблемы с параметрами
13	Запрос отметки времени
14	Ответ отметки времени

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Ошибка фрагментации
5	Ошибка в маршруте источника
6	Сеть назначения неизвестна
7	Узел назначения неизвестен
8	Узел-источник изолирован
9	Административный запрет



Транспортный уровень

Задача - передача данных между процессами на хостах.

- Адресация
- Надежность передачи данных

Сквозное соединение между двумя хостами
(уровень сетенезависимый)

Появился **интерфейс сокетов**



Гарантия доставки данных:

Подтверждение получения

Повторная отправка неподтвержденных данных

Гарантия порядка следования сообщений -
нумерация

Для адресации
используются
порты
192.168.1.3:80

Хорошо известные порты: 1-1024

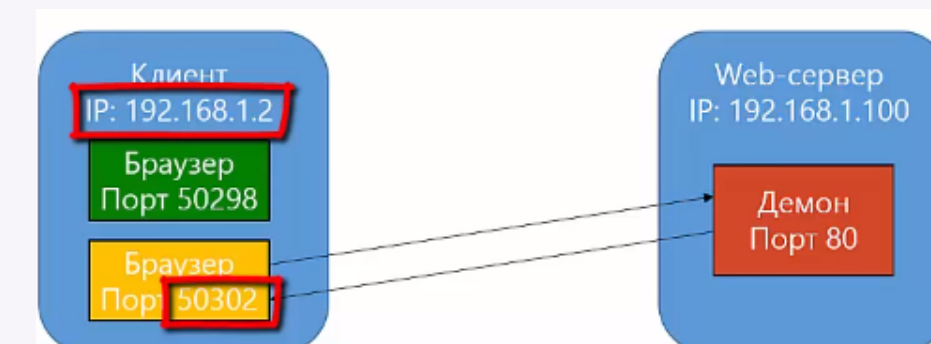
- 80 – HTTP (Web)
- 25 – SMTP (Электронная почта)
- 53 – DNS
- 67,68 – DHCP
- Использовать может только root/Администратор

Зарегистрированные порты: 1025-49151

- Регистрация в Internet Assigned Numbers Authority (IANA)

Динамические порты: 49151-65535

- Автоматически назначаются операционной системой сетевым приложениям



UDP

User Datagram Protocol

Сообщение UDP называется дейтаграмма

Задача - указывает порт отправителя и порт получателя

Особенности

Нет соединения - **фрагменты данных могут потеряться**

Нет гарантии доставки

Нет гарантии порядка сообщений

Преимущество - Скорость работы **быстрее** чем у TCP

Область применения:

клиент - сервер

короткие запросы -ответы

Пример: запрос IP- адреса у системы DNS

Стримы, вебинары, звонки по скайпу - общение в реальном времени

-
-
-
-
-
-
-
-
-
-
-

TCP

Transmission Control Protocol (протокол управления передачей)

Надежная передача потока байт. Обеспечивает **целостность данных.**

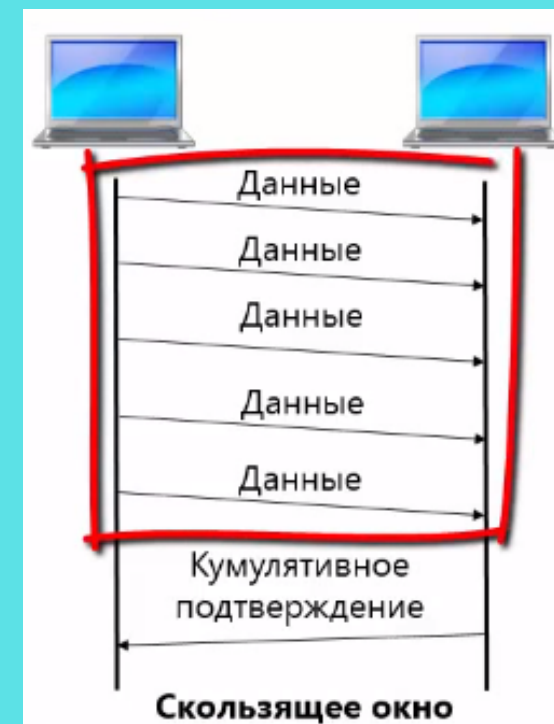
- гарантия доставки

подтверждение получения сообщения

повторная отправка при отсутствии

- гарантия сохранения порядка сообщений - нумерация сообщений (защита от дублирования)

Перед отправкой TCP должен установить соединение - трехстороннее рукопожатие (SYN - SYN ACK - ACK)



NAT - Network Address Translation

настройка PAT (Port Address Translation)

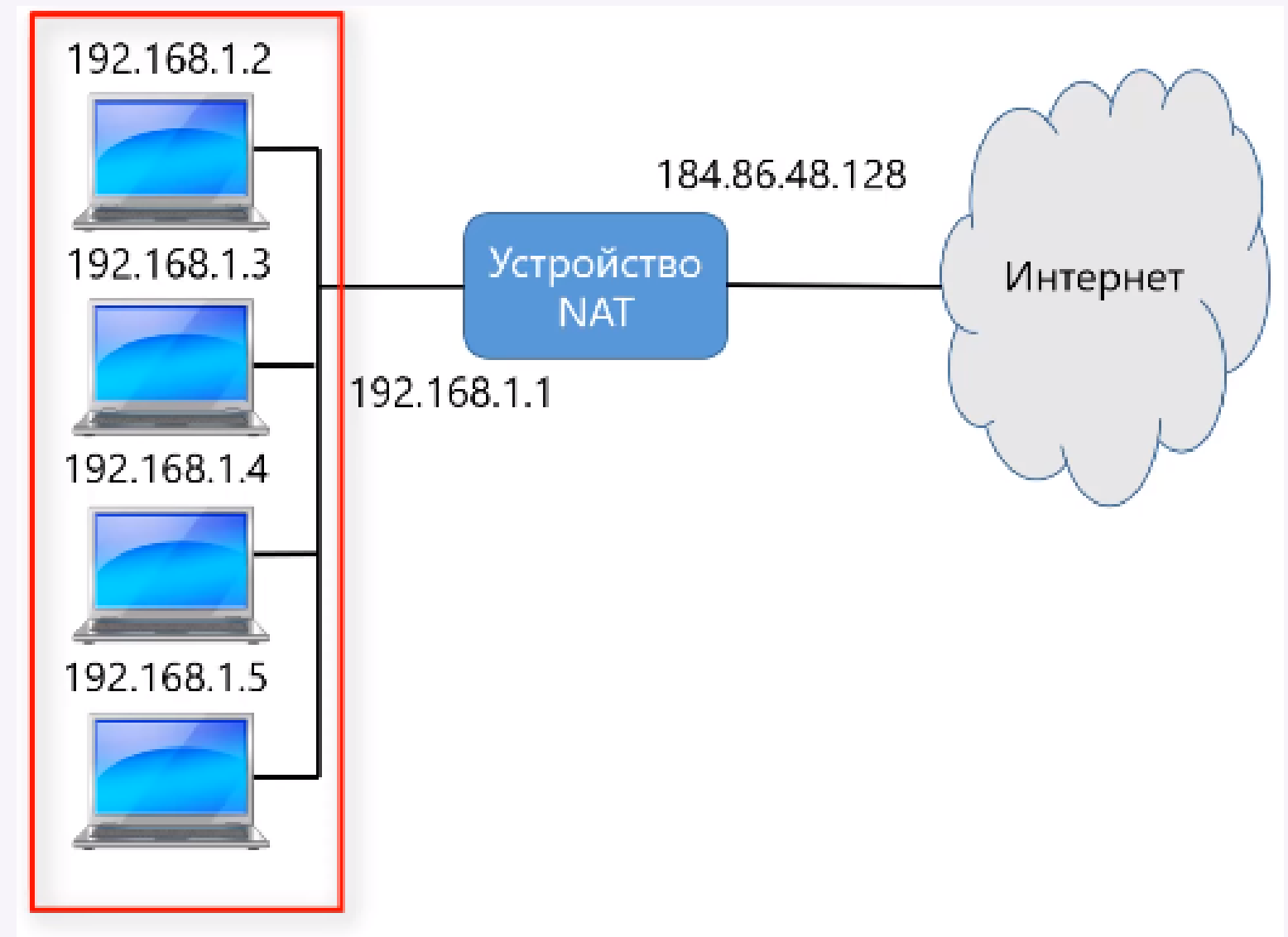
Технология преобразования IP-адресов внутренней сети (частной) в IP-адреса внешней сети (Интернет)

Причина - нехватка адресов IPv4

Внутренний адрес выдает провайдер, с ним мы находимся внутри локальной сети

Внешний адрес выдает провайдер для выхода в интернет, к нему добавляется порт - дополнительный идентификатор

• • • • •
• • • • •
• • • • •



Сеансовый уровень

Сеанс (сессия) - набор связанных сетевых взаимодействий, направленных на решение одной задачи

Отвечает за поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время.

Пример - загрузка веб-страницы

Уровень представления

Кодирование и сжатие

Происходит преобразование форматов при переходе с одного уровня на другой. Пример - при передаче фото на нижний уровень оно превращается в 0 и 1. На обратном пути снова собирается в изображение.

Для защиты передаваемых по сети данных используется шифрование : SSL, TLS. Шифрование также происходит на этом уровне.

Уровень приложения (Прикладной)

Отвечает за взаимодействие сетевых приложений. Пример - браузер

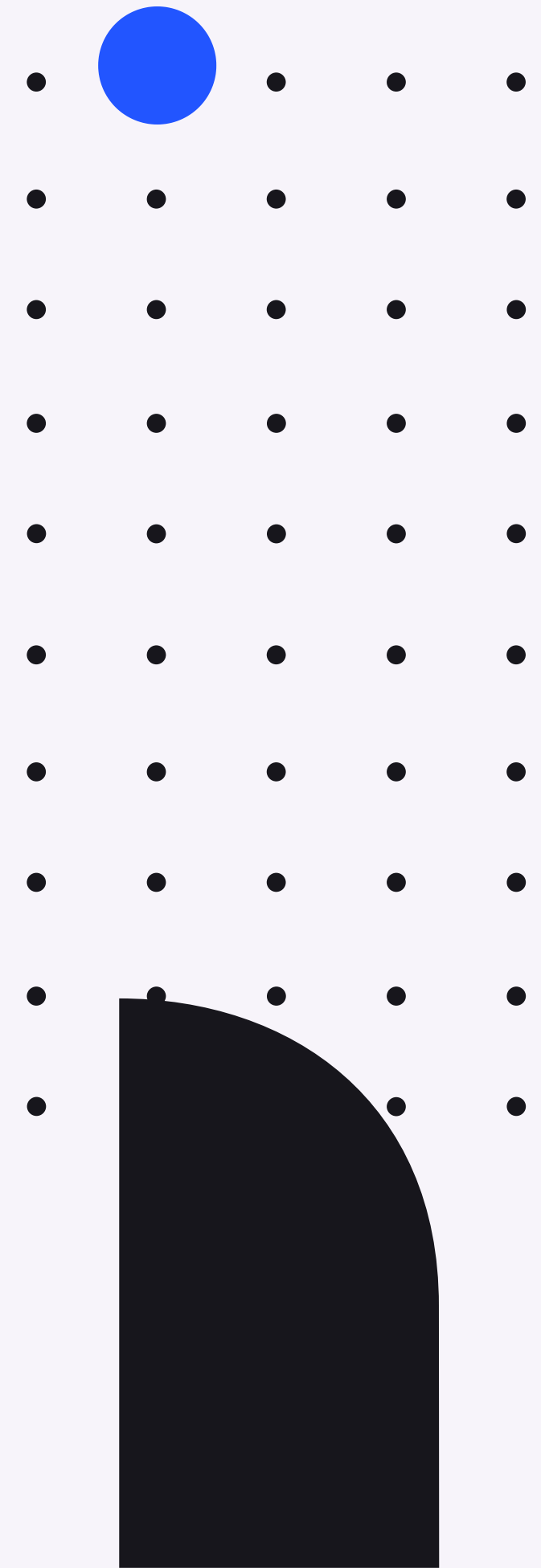
Протоколы прикладного уровня:

HTTP

SMTP, POP3, IMAP,

DNS,

FTP



DNS - Domain Name Systems

Система доменных имен позволяет использовать вместо IP-адресов понятные человеку символьные имена компьютеров
также позволяет по этому имени определить IP-адрес

Если компания захочет перенести свой сервер на другой компьютер с другим IP-адресом, то доменное имя не изменится

Режимы работы:

итеративный - если сервер не отвечает за ту зону, на которую пришел запрос, то он присылает адрес другого сервера, к которому нужно обратиться
рекурсивный (DNS resolver) - сервер сам отправляет запросы другим серверам пока не найдет нужную инфу и не вернет ее клиенту

Типы ответов

авторитетный - ответ от сервера, который является ответственным за эту зону

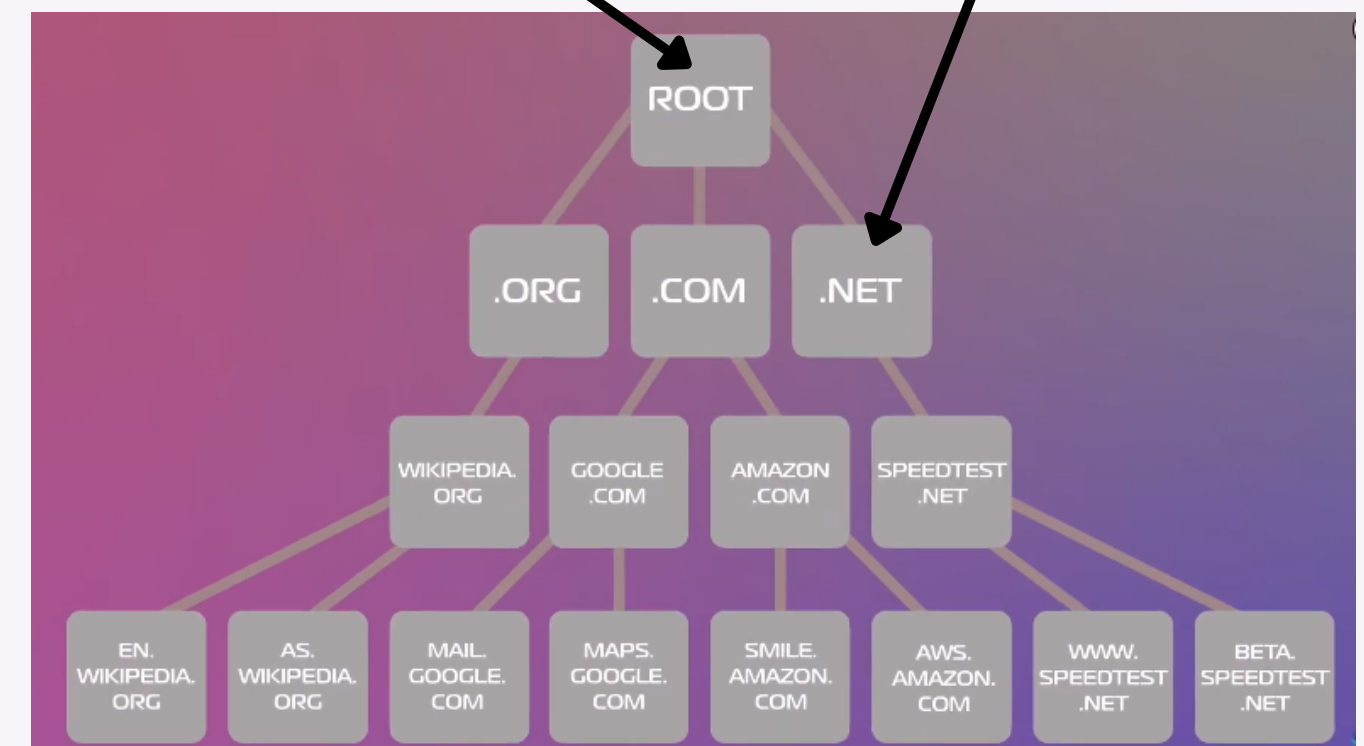
неавторитетный - от другого сервера (например resolver, который ранее закэшировал инфу)

утилита nslookup позволяет найти IP-адрес по доменному имени

```
C:\Users\alena>nslookup www.yandex.ru
ТхЕтхЕ:  cache-gr2.grodno.by
Address:  86.57.160.66

Не заслуживающий доверия ответ:
Ль :      www.yandex.ru
Addresses: 2a02:6b8:a::a
           77.88.55.80
           5.255.255.80
           5.255.255.88
           77.88.55.88
```

корневой сервер домен первого уровня



HTTP - протокол передачи гипертекста



URL - уникальный адрес веб страницы в интернете

HTTP работает в режиме запрос-ответ

Протокол транспортного уровня **TCP**

Порт сервера - **80**



Есть несколько версий протокола HTTP

HTTP 1 - первая официальная версия, 1996

HTTP 1.1 - расширение первой версии, 1997

- кэширование, keep-alive, аутентификация

HTTP 2.0



- использует бинарный формат (0 и 1), влияет на производительность

- сжатие заголовков

- все запросы походят по одному TCP соединению

Протокол поддерживает работу кэша

Кэширование позволяет сократить время загрузки

Веб-страницы, изображения, таблицы стилей

Кэширование позволяет сократить время загрузки Web-страниц

- Ресурсы загружаются из кэша, а не с сервера

Можно ли использовать копию ресурса из кэша?

- Заголовок Expires
- Заголовок Cache-Control

Запрос Get с условием:

- Заголовок If-Modified-Since (по дате)
- Заголовок If-None-Match (по ETag)

Тип кэша:

- Частный: в браузере
- Разделяемый (proxy, reverse proxy и др.)

FTP File Transfer Protocol

1

Протокол передачи файлов

Один из самых старых

Работает в режиме клиент-сервер

Работает с файловой системой на FTP-сервере

Для адресации файлов также использует URL

2

Протокол FTP использует 2 соединения

- управляющее - открыто всё время работы

- передачи данных - инициируется со стороны сервера

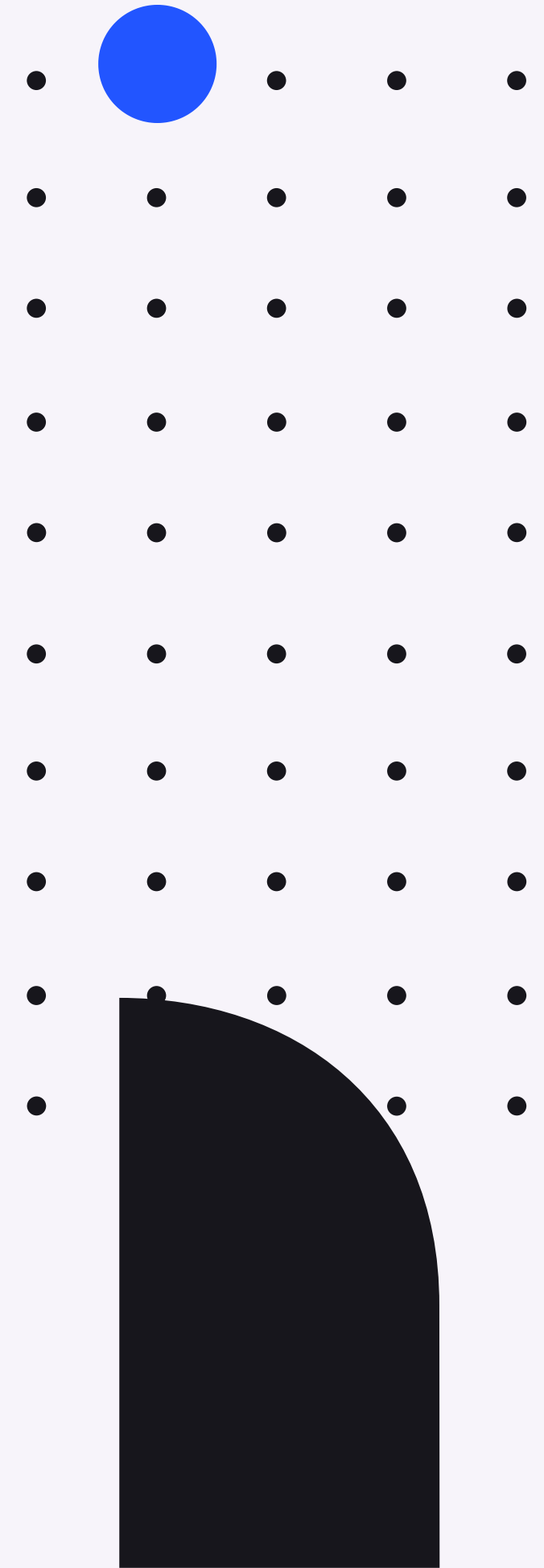
Недостатки

- проблема с NAT и межсетевыми экранами

- низкая безопасность - id и пароль передаются по сети в открытом виде

3

используется замена FTP на основе SSH - SFTP



Протоколы Электронной почты

1

Протокол SMTP

Simple Mail Transfer Protocol

Используется для передачи сообщений от агента пользователя почтовому серверу и между серверами

2

Протокол POP3

Post Office Protocol 3

Используется для чтения писем из хранилища сообщений. Передает все сообщения из хранилища на локальный компьютер пользователя и только после этого показывает их в агенте. Удаляет с сервера все сообщения, которые были получены пользователем

3

Протокол IMAP

Internet Message Access Protocol

Рассчитан на работу напрямую с хранилищем сообщений. Письма после почтения пользователем не удаляются из хранилища.

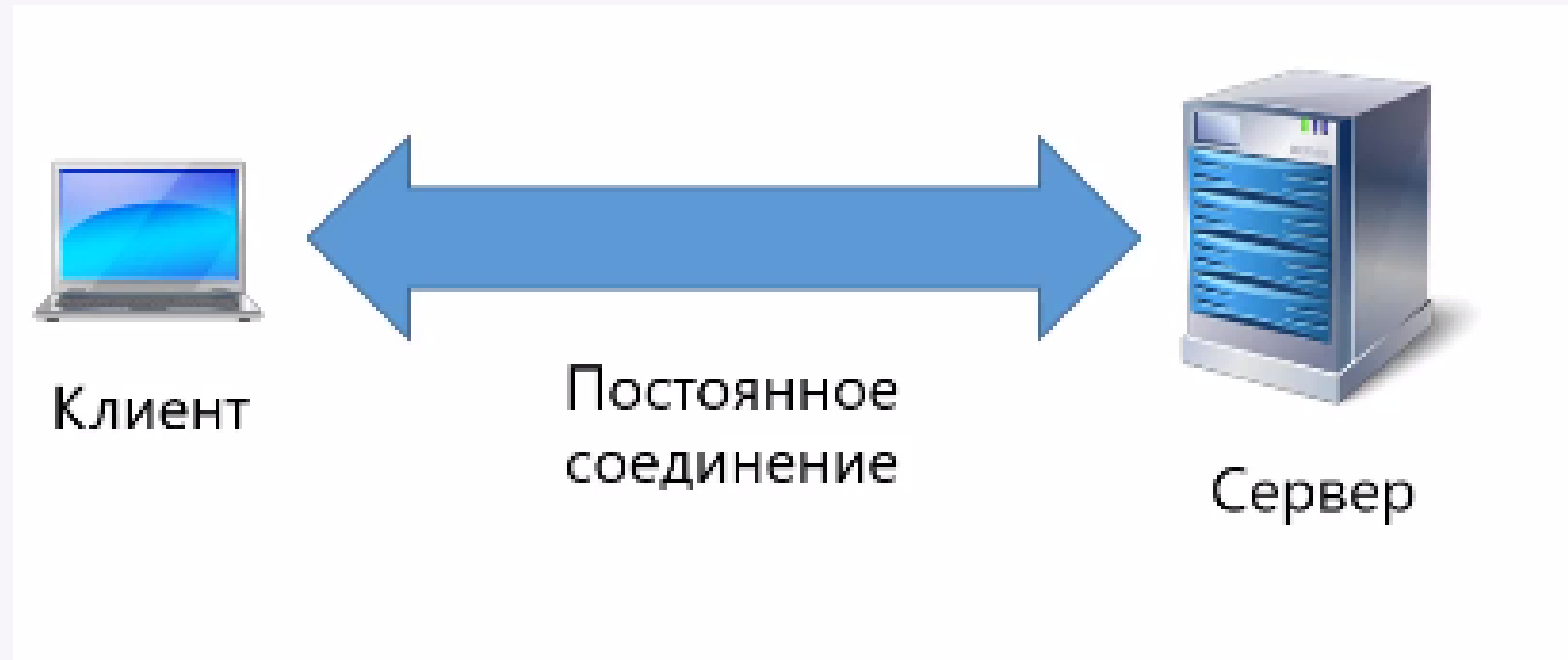
С почтовым ящиком может работать сразу несколько клиентов

Могут быть разные папки. Есть флаги.

Все протоколы работают в текстовом режиме
Взаимодействие запрос-ответ



Протокол WS (Web сокет)



Между клиентом и сервером устанавливается постоянное двунаправленное соединение
Сервер может отправлять данные по своей инициативе
Пример- чаты

Установка соединения: запрос и ответ

2

```
GET /chat HTTP/1.1
Host: www.asozykin.ru
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: dGhlIHhnbXBsZSBub25jZQ==
Origin: http://asozykin.ru
Sec-WebSocket-Version: 13
```

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: s3pPLMBiTxaQ9kYGzzhZRbK+x0o=
```

3

Данные передаются в виде кадров через соединение TCP (заголовки кадров бинарные, что снижает накладные расходы)

Есть фрагментация

Типы кадров - текстовые данные (кодировка UTF-8), бинарные данные, управляющие кадры