

М

Т

# ОСНОВЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

С

# Содержание модуля

1. Роль протоколов в компьютерных сетях
2. Стеки протоколов
3. Основные функции протоколов
4. Основные протоколы TCP/IP

# Основные протоколы TCP/IP

4

# Стек TCP/IP

## Модель TCP/IP

Уровень приложений/прикладной  
(Application)

Транспортный уровень  
(Transport)

Межсетевой уровень  
(Internet)

Уровень доступа к сети  
(Network Access)

## Набор протоколов TCP/IP

Разрешение имен: **DNS**

Протокол с установлением соединения: **TCP**  
Без установления соединения: **UDP**

Интернет протоколы: **IPv4, IPv6, NAT**  
Обмен сообщениями: **ICMPv4, ICMPv6**

Разрешение адресов: **ARP**  
Протоколы канального уровня: **Ethernet, VLAN**

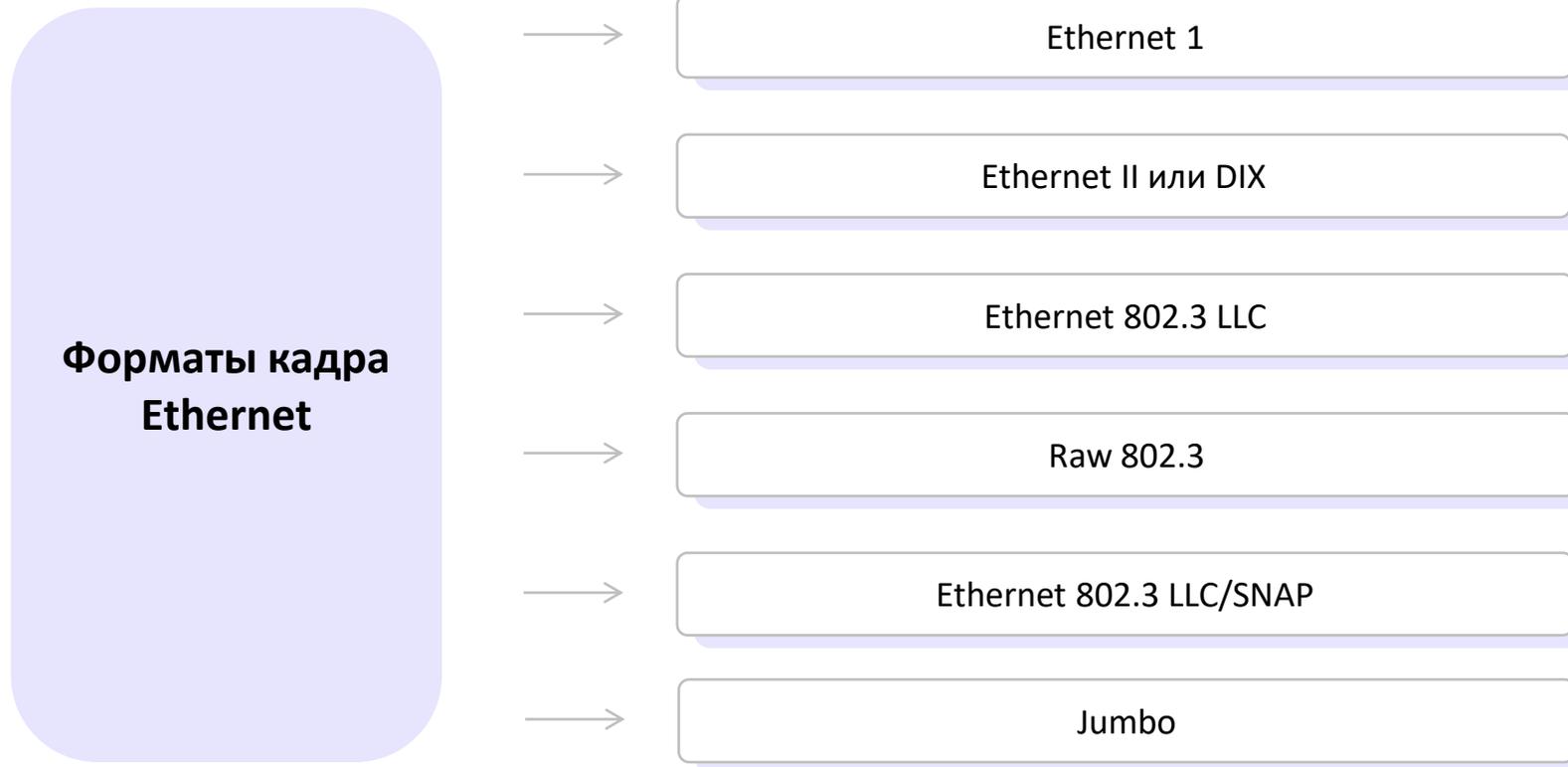
# Справка по протоколу Ethernet

- Изобретен в 1973 в Xerox PARC
- Протокол канального уровня
- Изначально в качестве передающей среды использовался коаксиальный кабель
- Сегодня может использоваться витая пара, оптические кабели и радиоэфир
- Описывается набором стандартов IEEE 802.3

# Принцип работы Ethernet



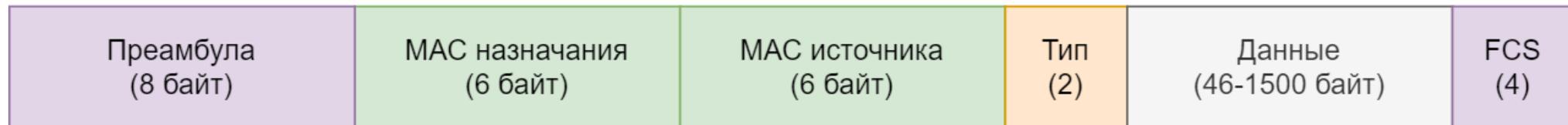
# Версии Ethernet



# Справка по протоколу Ethernet

Ethernet II - Наиболее распространённый формат кадра Ethernet

## Кадр Ethernet II



# Альтернативы Ethernet II

## RAW 802.3

Преамбула (7 байт)	SFD (1)	MAC назначения (6 байт)	MAC источника (6 байт)	Длина (2)	Данные (46-1500 байт)	FCS (4)
-----------------------	------------	----------------------------	---------------------------	--------------	--------------------------	------------

## 802.3 LLC

Преамбула (7 байт)	SFD (1)	MAC назначения (6 байт)	MAC источника (6 байт)	Длина (2)	LLC (3)	Данные (46-1497 байт)	FCS (4)
-----------------------	------------	----------------------------	---------------------------	--------------	------------	--------------------------	------------

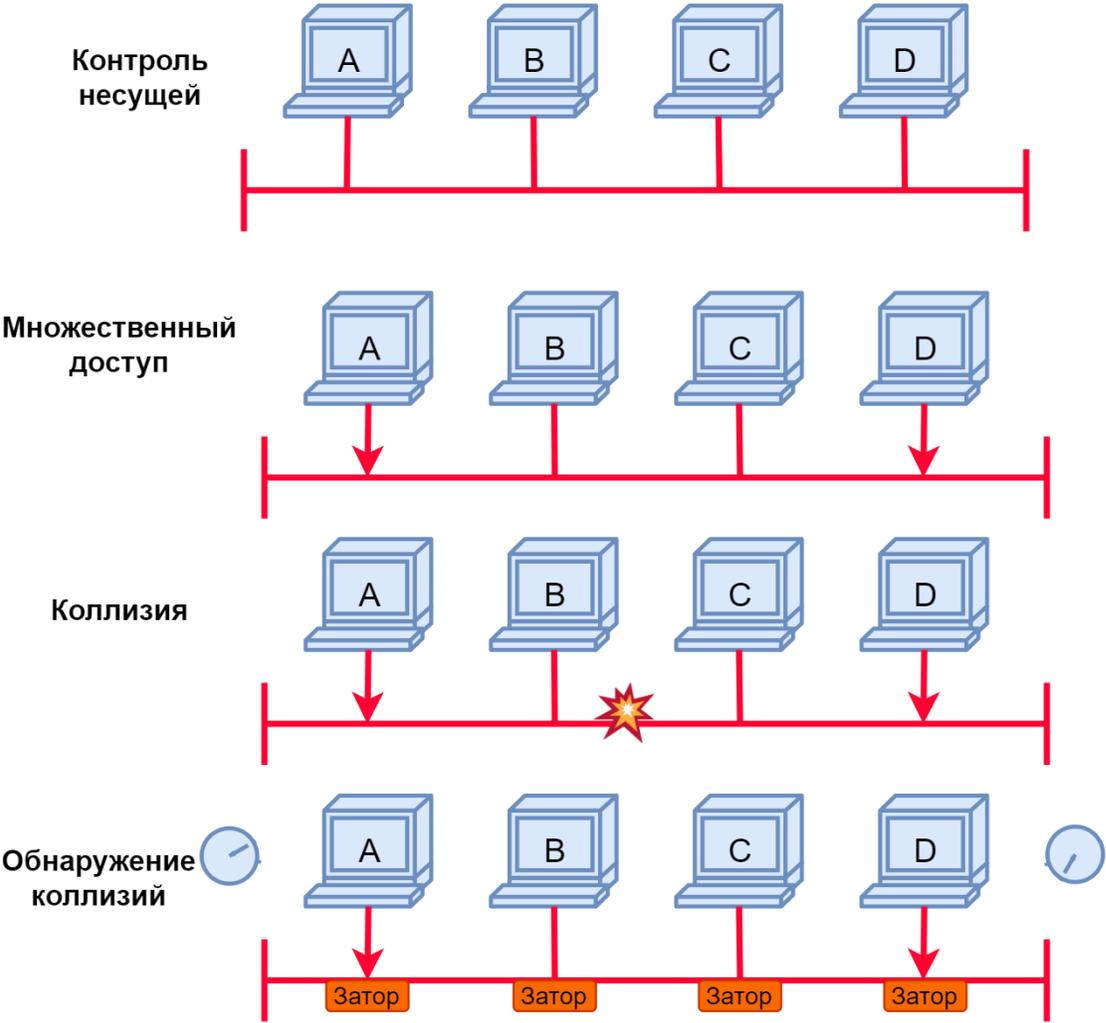
## 802.3 LLC/SNAP

Преамбула (7 байт)	SFD (1)	MAC назначения (6 байт)	MAC источника (6 байт)	Длина (2)	LLC (3)	SNAP (5)	Данные (46-1492 байт)	FCS (4)
-----------------------	------------	----------------------------	---------------------------	--------------	------------	-------------	--------------------------	------------

## Jumbo

Преамбула (7 байт)	MAC назначения (6 байт)	MAC источника (6 байт)	Тип (2)	Данные (46-9000 байт)	FCS (4)
-----------------------	----------------------------	---------------------------	------------	--------------------------	------------

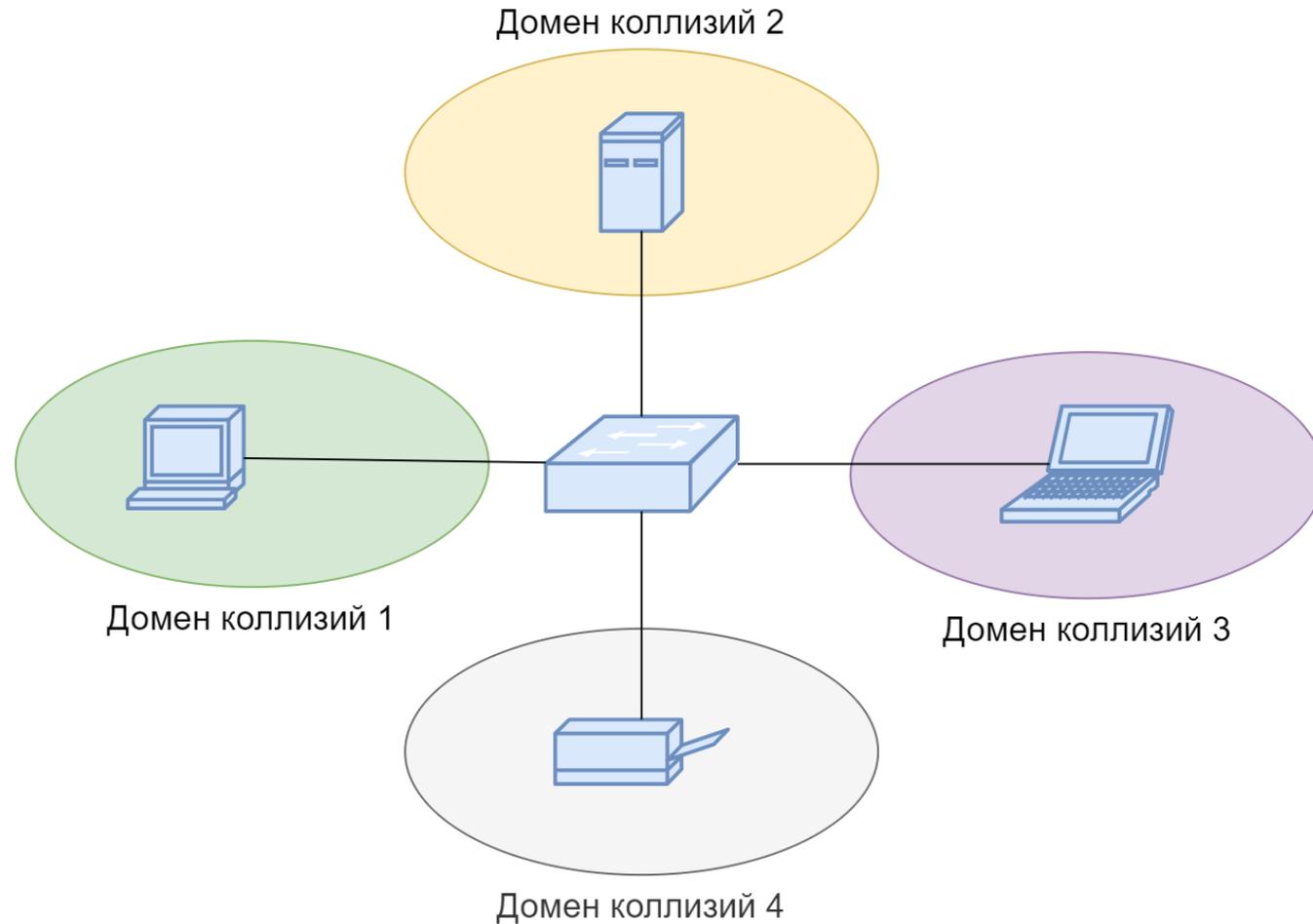
# Метод доступа CSMA/CD



# Проблемы CSMA/CD

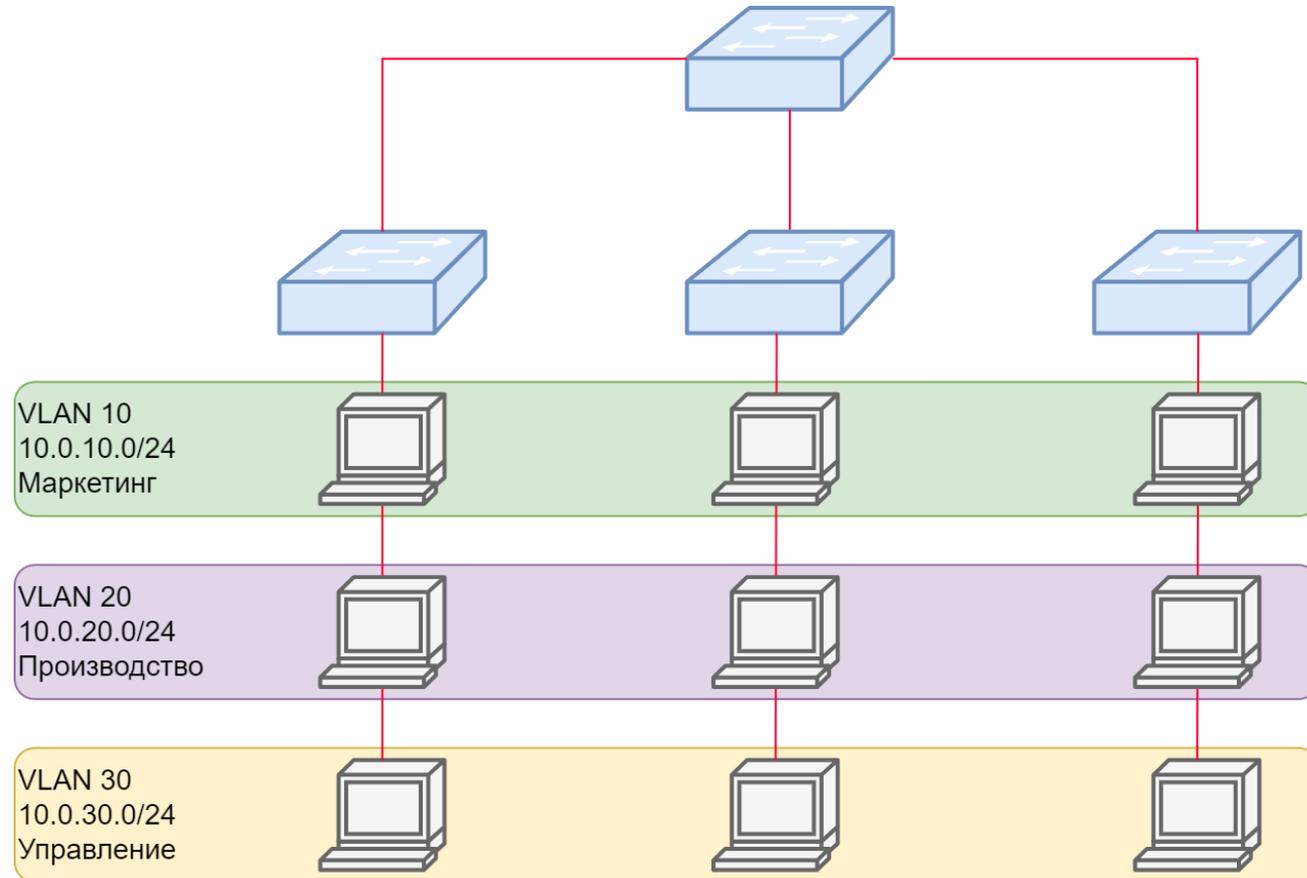
- Устройство может или передавать, или принимать данные (Half Duplex)
- При увеличении количества узлов растет вероятность возникновения коллизий
- Увеличение числа коллизий снижает доступную ширину полосы пропускания для полезного трафика

# Решение проблем CSMA/CD посредством коммутаторов



# Логическое деление сети с помощью VLAN

- VLAN – Virtual Local Area Network
- Сегментация
- Гибкость
- Безопасность



# Логическое деление сети с помощью VLAN

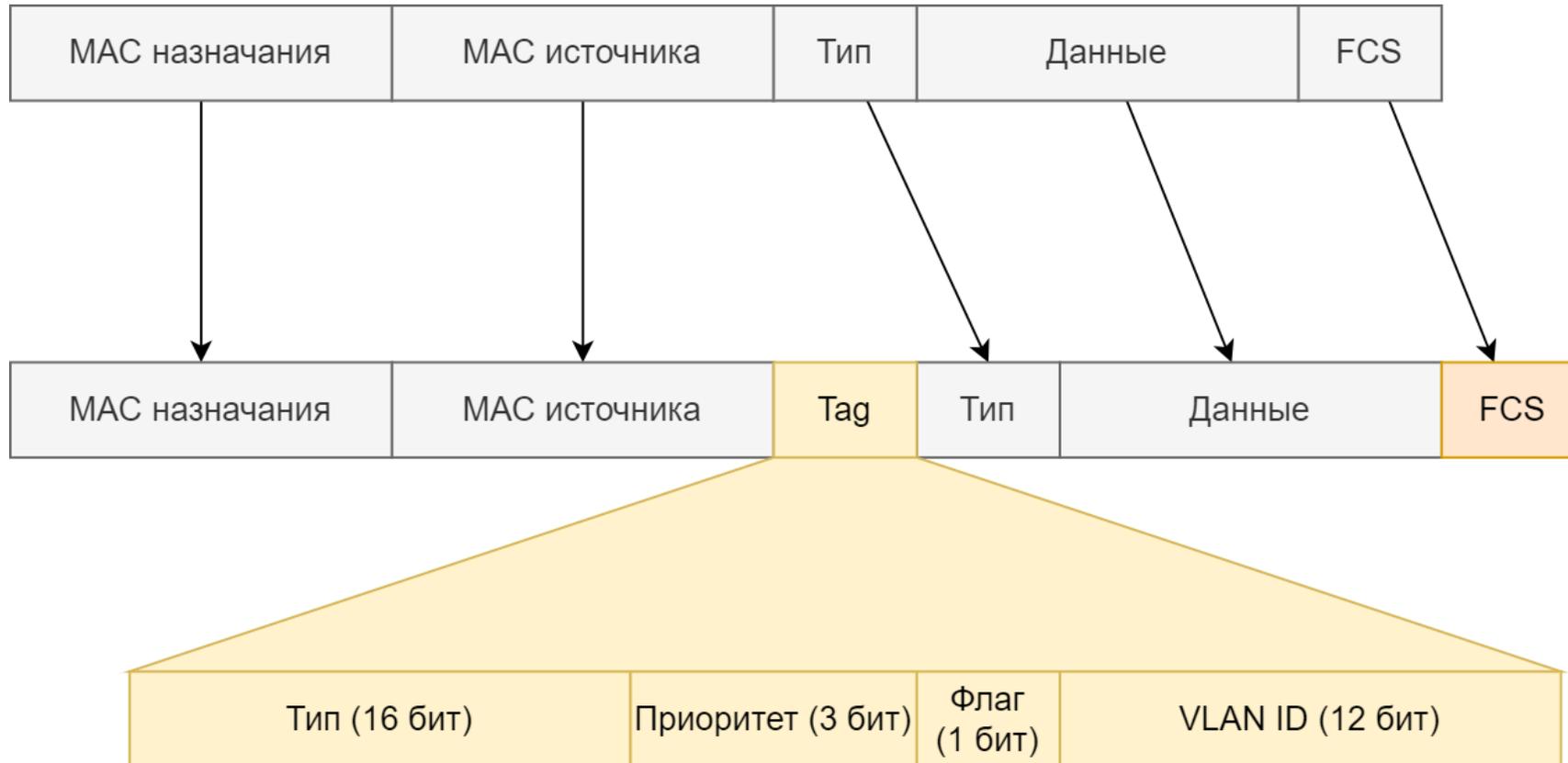
- VLAN = широковещательный домен
- VLAN = логическая подсеть



# Логическое деление сети с помощью VLAN



# Тегирование кадров Ethernet (802.1Q)



# Internet Protocol v4

## Свойства протокола



Работает на межсетевом уровне



Не устанавливает соединений



Пакеты обрабатываются независимо



Иерархическая адресация устройств



Не гарантирует доставку данных



Не восстанавливает данные

# Заголовок IPv4

Версия 4-бита	Длина заголовка 4-бита	Тип услуги 8-бит	Длина пакета 16-бит	
Идентификатор 16-бит		Флаги 3-бита	Сдвиг фрагмента 13-бит	
Время жизни 8-бит	Протокол 8-бит		Контрольная сумма заголовка 16-бит	
Адрес источника 32-бита				
Адрес назначения 32-бита				
Опции от 0 до 40 байт				Заполнитель
Данные				

# IP адрес

- Однозначно определяет каждое устройство в сети
- Должен быть уникальным
- Записывается в виде четырех десятичных чисел от 0 до 255 (10.1.222.3)
- Состоит из двух частей:
  - Идентификатор сети
  - Идентификатор узла

Идентификатор сети

Идентификатор узла

# Формирование IP адреса

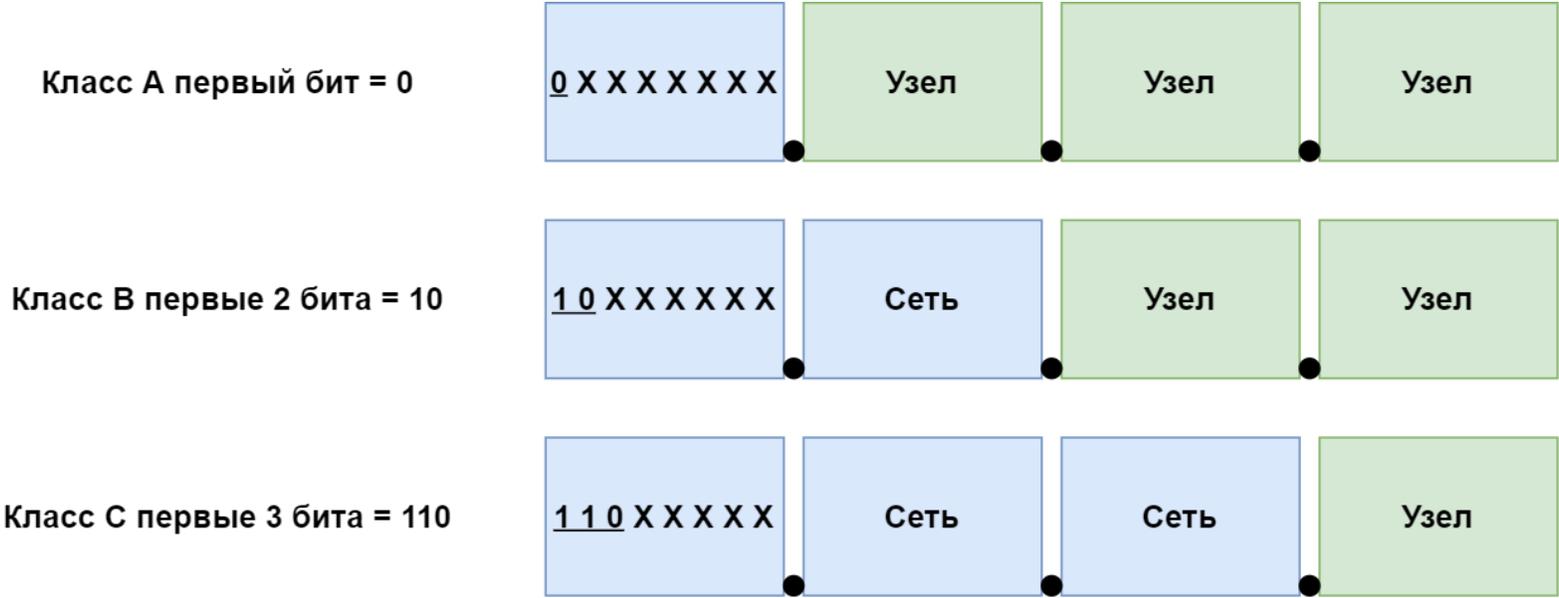


двойка в степени	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
значения степени двойки	128	64	32	16	8	4	2	1
первый октет (192)	1	1	0	0	0	0	0	0

$192 = 2^7 + 2^6 = 128 + 64$        $168 = 2^7 + 2^5 + 2^3 = 128 + 32 + 8$  и т.д.

# Классы IP адресов

**Классы –**  
 ранний способ определения сетевой и узловой части адреса IPv4



# Адрес сети и широковещательный адрес

		Сетевая часть	Хостовая часть
IPv4-адрес	192 . 168 . 10 . 10	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 .	0 0 0 0 1 0 1 0
IPv4-адрес сети	192 . 168 . 10 . <b>0</b>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 .	<b>0 0 0 0 0 0 0 0</b>
Широковещательный адрес	192 . 168 . 10 . <b>255</b>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 .	<b>1 1 1 1 1 1 1 1</b>
Первый доступный адрес	192 . 168 . 10 . <b>1</b>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 .	<b>0 0 0 0 0 0 0 1</b>
Последний доступный адрес	192 . 168 . 10 . <b>254</b>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 .	<b>1 1 1 1 1 1 1 0</b>

Кол-во доступных адресов =  $2^n - 2$ , где n - кол-во бит в хостовой части

Кол-во доступных адресов для сети 192.168.10.0 =  $2^8 - 2 = 254$

# Подсети

## Свойства



Трехуровневая структура адреса



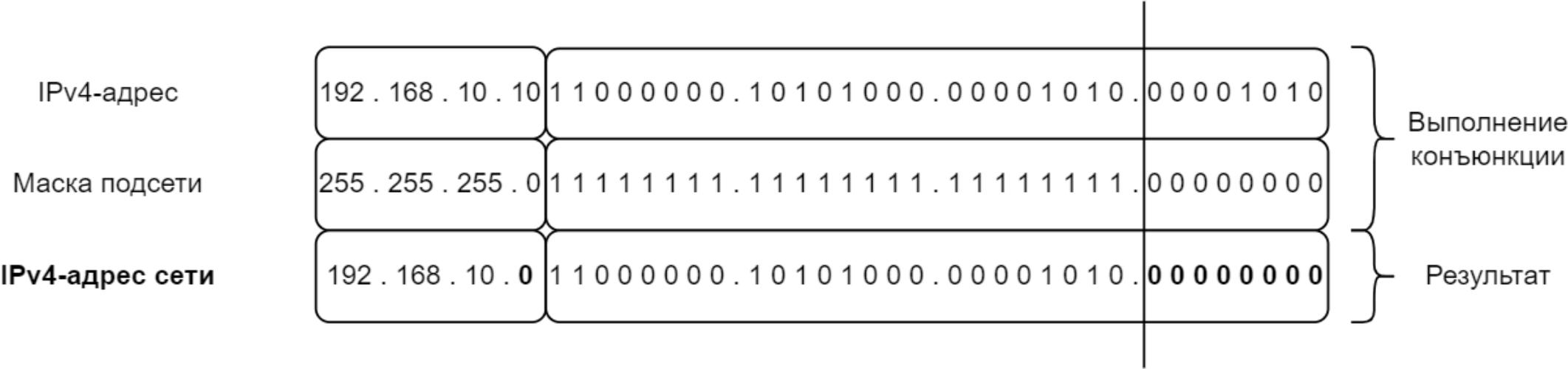
Более эффективное использование адресного пространства



Вводится понятие сетевой маски

# Сетевая маска

- Отделяет в адресе номер сети от номера узла
- Непрерывная последовательность битов 1 – определяет биты сети
- Непрерывная последовательность битов 0 – биты узла



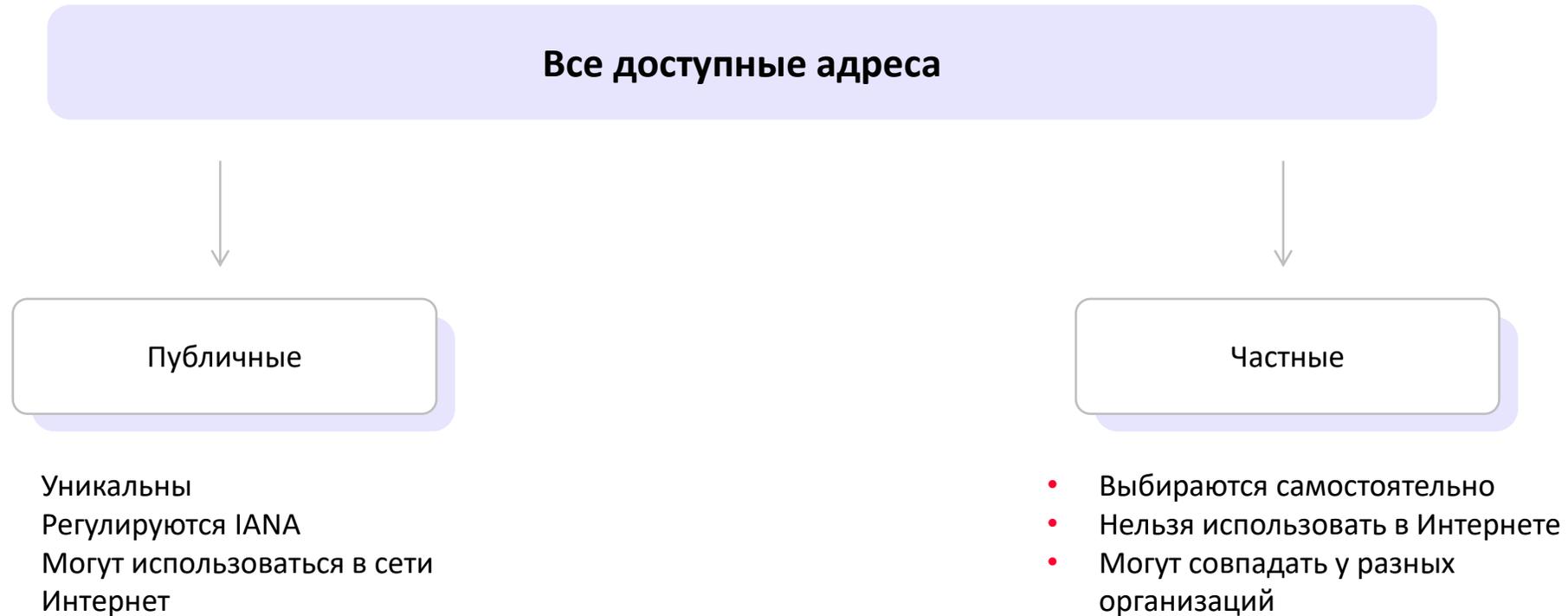
# Подсети с фиксированной маской

Исходная сеть	172. 16. 0. 0	10101100.00010000	000000	00.00000000
Маска исходной сети	255.255. 0. 0	10101100.00010000	000000	00.00000000
Маска подсети	255.255.252. 0	10101100.00010000	111111	00.00000000
IPv4-адрес подсети №1	172. 16. 0. 0	10101100.00010000	000000	00.00000000
Первый используемый IPv4-адрес	172. 16. 0. 1	10101100.00010000	000000	00.00000001
Последний используемый IPv4-адрес	172. 16. 3.254	10101100.00010000	000000	11.11111110
Широковещательный адрес подсети №1	172. 16. 3.255	10101100.00010000	000000	11.11111111
IPv4-адрес подсети №2	172. 16. 4. 0	10101100.00010000	000001	00.00000000
Первый используемый IPv4-адрес	172. 16. 4. 1	10101100.00010000	000001	00.00000001
Последний используемый IPv4-адрес	172. 16. 7.254	10101100.00010000	000001	11.11111110
Широковещательный адрес подсети №2	172. 16. 7.255	10101100.00010000	000001	11.11111111

# Современный способ деления адресного пространства

- Отказ от классов – Classless Inter Domain Routing (CIDR). Используются префиксы w.x.y.x/m
- Маски переменной длины – Variable Length Subnet Mask (VLSM)

# Частные и публичные адреса



# Диапазоны адресов

Публичные	Частные
1.0.0.0-9.255.255.255 11.0.0.0-126.0.0.0	10.0.0.0-10.255.255.255
128.1.0.0-172.15.255.255 172.32.0.0-191.254.255.255	172.16.0.0-172.31.255.255
192.0.1.0-192.167.255.255 192.169.0.0-223.255.255.255	192.168.0.0-192.168.255.255

# Специальные адреса

## Виды адресов

- Не назначенный – 0.0.0.0
- Замыкания на себя (loopback) – 127.0.0.0-127.255.255.255
- Марсианские – 0.0.0.1-0.255.255.255, 128.0.0.0-128.0.255.255, 191.255.0.0-191.255.255.255, 192.0.0.0-192.0.0.255, 223.255.255.0-223.255.255.255
- Резервированные – 240.0.0.0-255.255.255.254
- Групповой рассылки – 224.0.0.0-239.255.255.255

# Ограничения протокола IPv4

- Ограниченное адресное пространство ( $2^{32} \sim 4$  млрд)
- Не эффективное распределение
- Сложная обработка заголовка – переменная длина и контрольная сумма



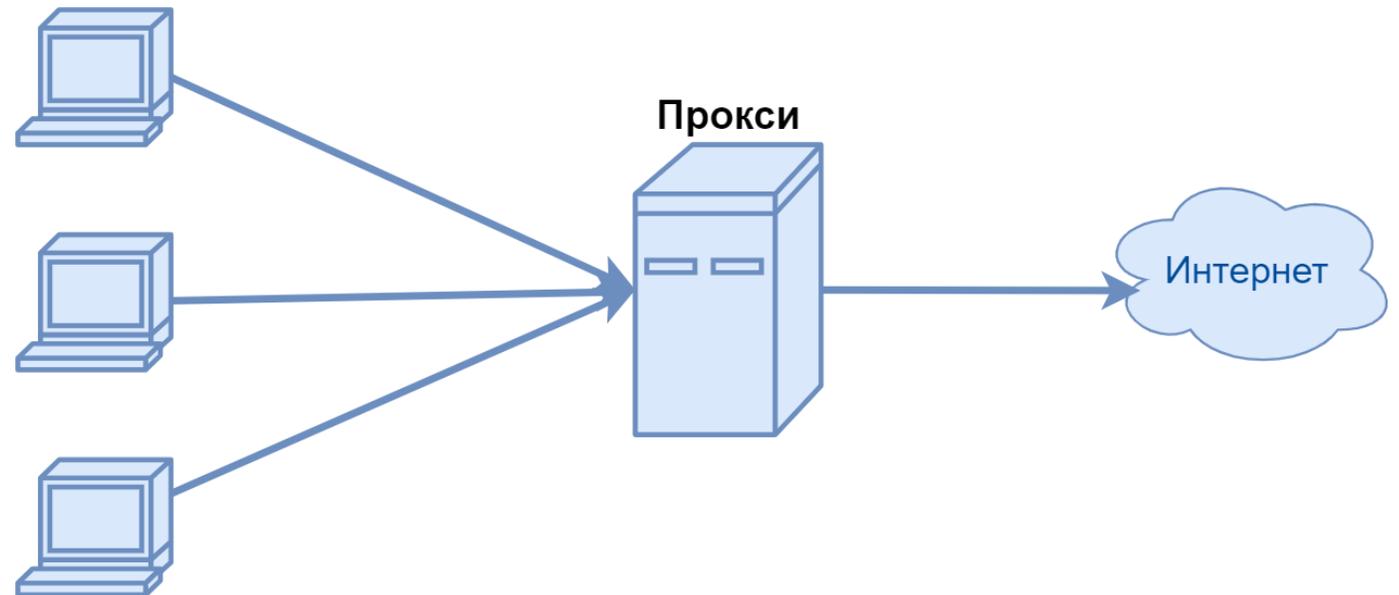
# Способы преодоления ограничений

- Использование прокси серверов
- Применение трансляции сетевых адресов
- Переход на новый протокол IPv6

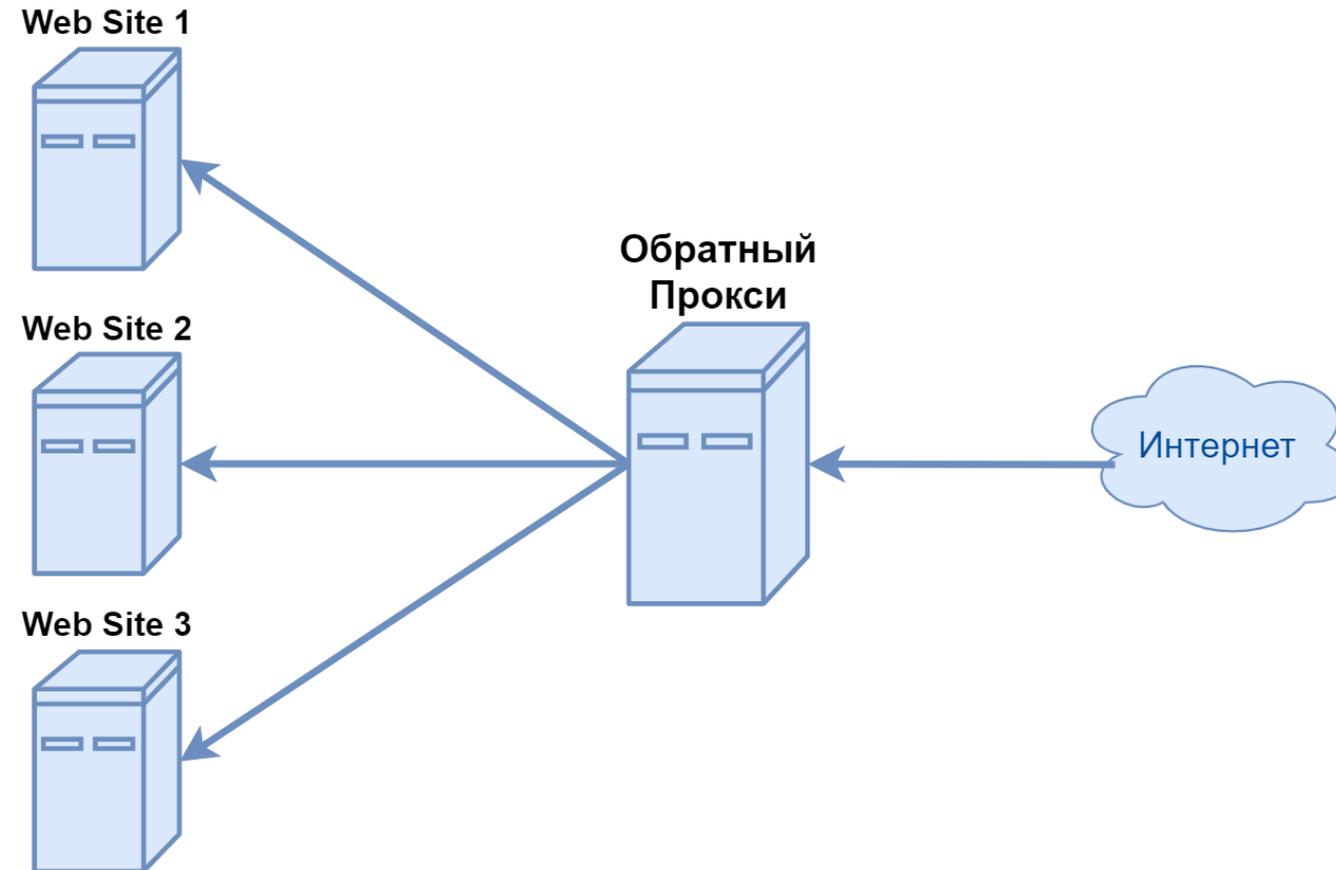


# Прокси

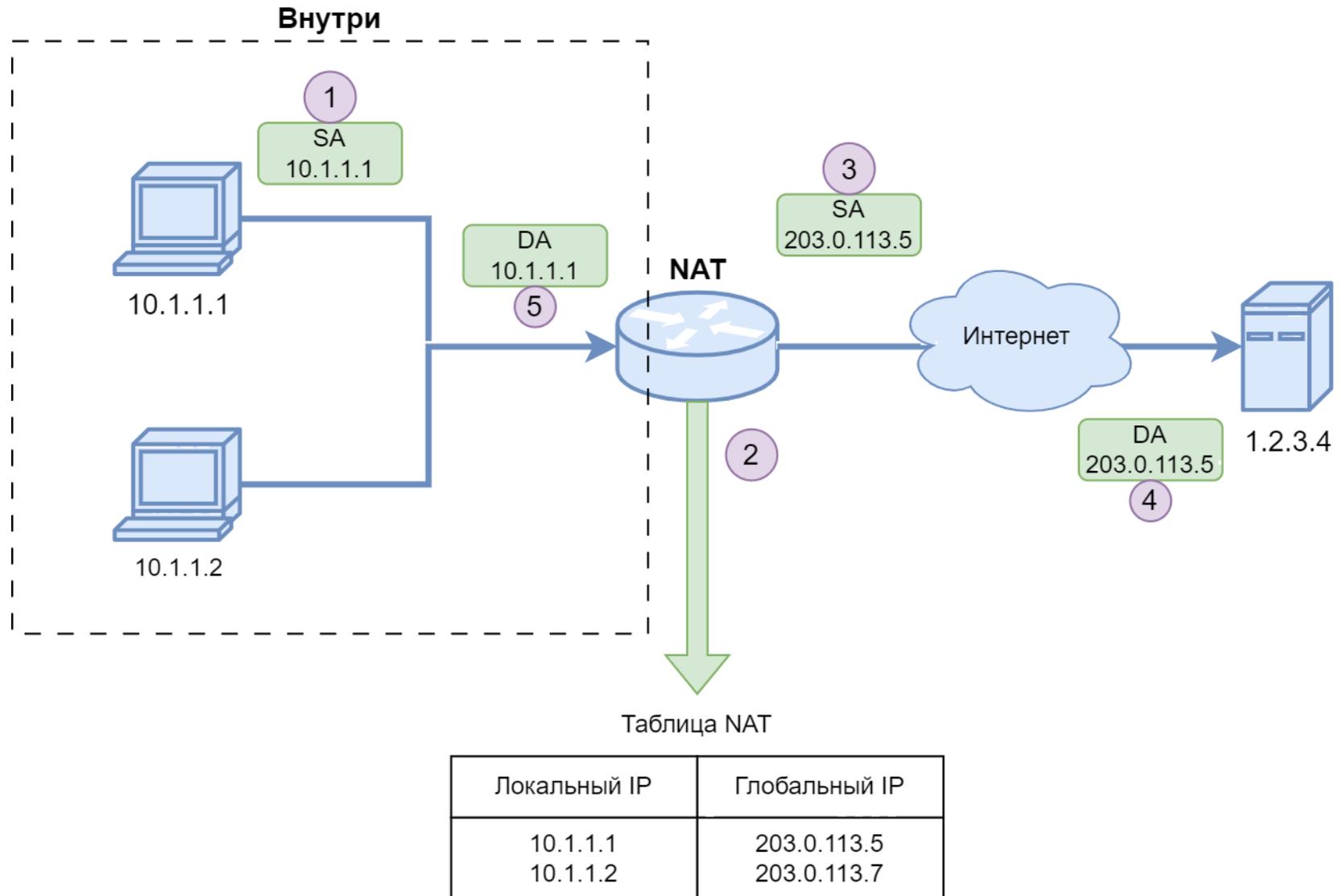
Клиент делает запрос к прокси, сервер подключается к ресурсу в интернете и возвращает результат клиенту



# Обратный прокси



# Трансляция сетевых адресов (NAT)



# Трансляция портов (PAT)

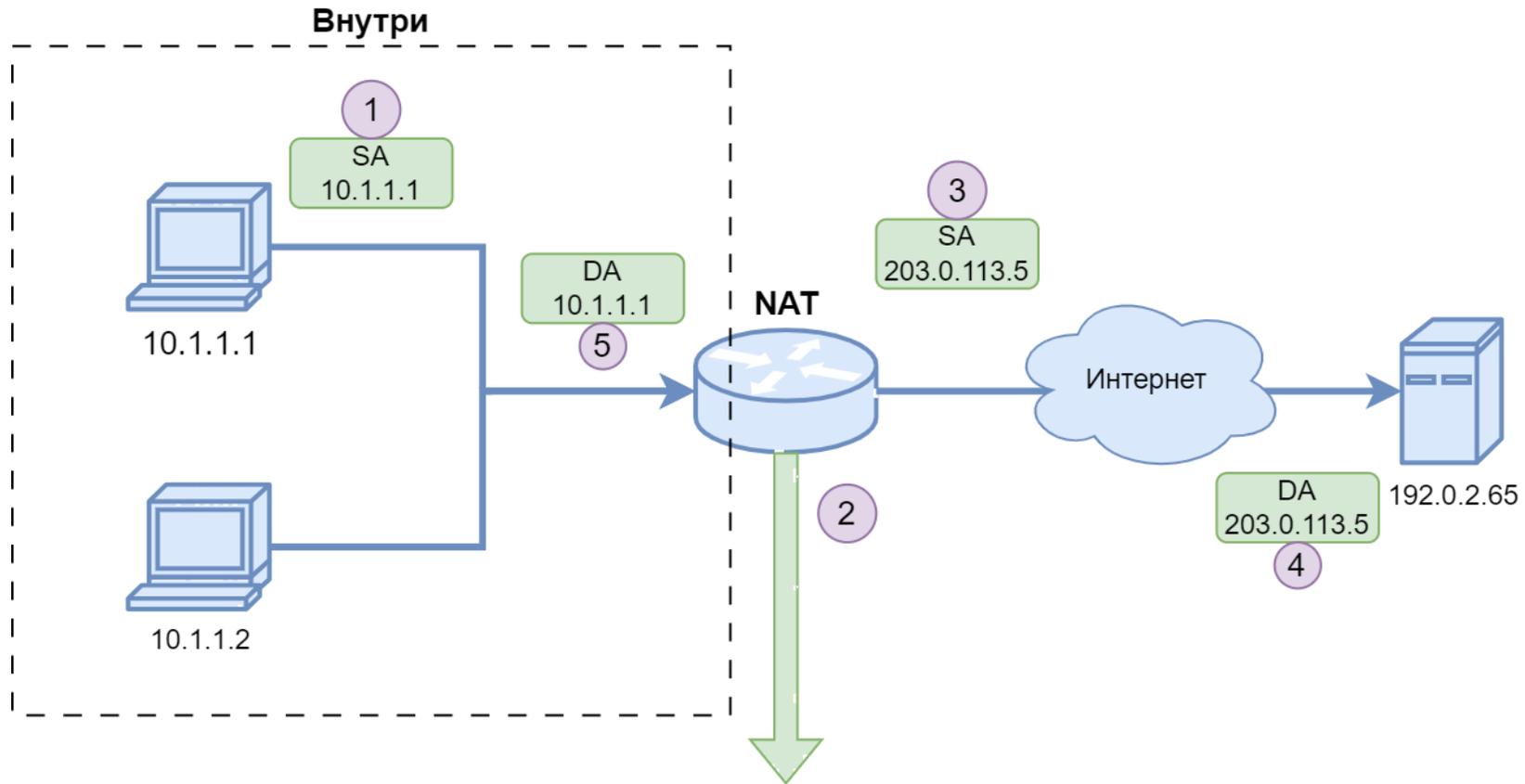


Таблица NAT

Протокол	Локальный IP:Порт	Глобальный IP:Порт	Внешний Глобальный IP:Порт
TCP	10.1.1.1:1234	203.0.113.5:1234	192.0.2.65:80
TCP	10.1.1.2:4321	203.0.113.5:4321	192.0.2.65:80

# IPv6

- Увеличенное адресное пространство ( $2^{128} \sim 3 \cdot 10^{38}$  адресов )
- Более простой заголовок
- Мобильность и безопасность
- Другие принципы разделения адресного пространства и выделения адресов
- Множество вариантов перехода

# Адрес IPv6

- 128-битное число
- Записывается в виде 8 блоков шестнадцатеричных чисел, разделенных символом «:»
- Начальные нули в блоке записывать не обязательно
- Блоки последовательных нулей можно заменить на «::», но только один раз

2001:0000:1230:0000:0000:0000:8F8F:0001



2001:0:1230:0:0:ABCD:8F8F:1



2001:0:1230::8F8F:1

0:0:0:0:0:0:0:1  $\Rightarrow$  ::1

# IPv6

## Типы адресов



Индивидуальные (unicast)



Групповые (multicast)



Альтернативный (anycast)

# Транспортные протоколы



## **TCP (Transmission Control Protocol) –**

обеспечивает надежную передачу данных между приложениями



## **UDP (User Datagram Protocol) –**

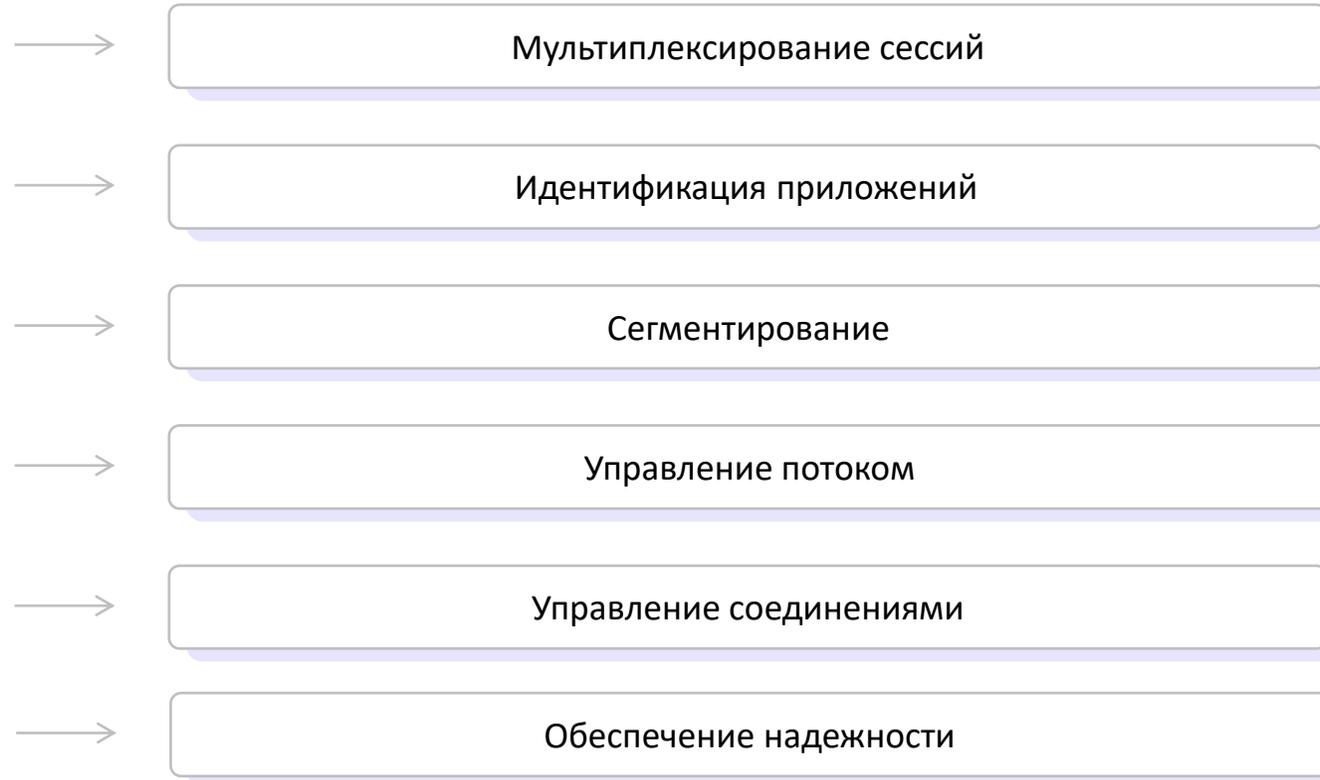
позволяет передавать данные между приложениями с минимальными накладными расходами, но без гарантии доставки

# Структура заголовка TCP

16-бит Порт источника		16-бит Порт назначения	
32-бит Последовательный номер			
32-бит Номер подтверждения			
4-бит Длина заголовка	Резерв	Флаги	16-бит Размер окна
16-бит Контрольная сумма		16-бит Указатель срочности	
Опции			
Данные			

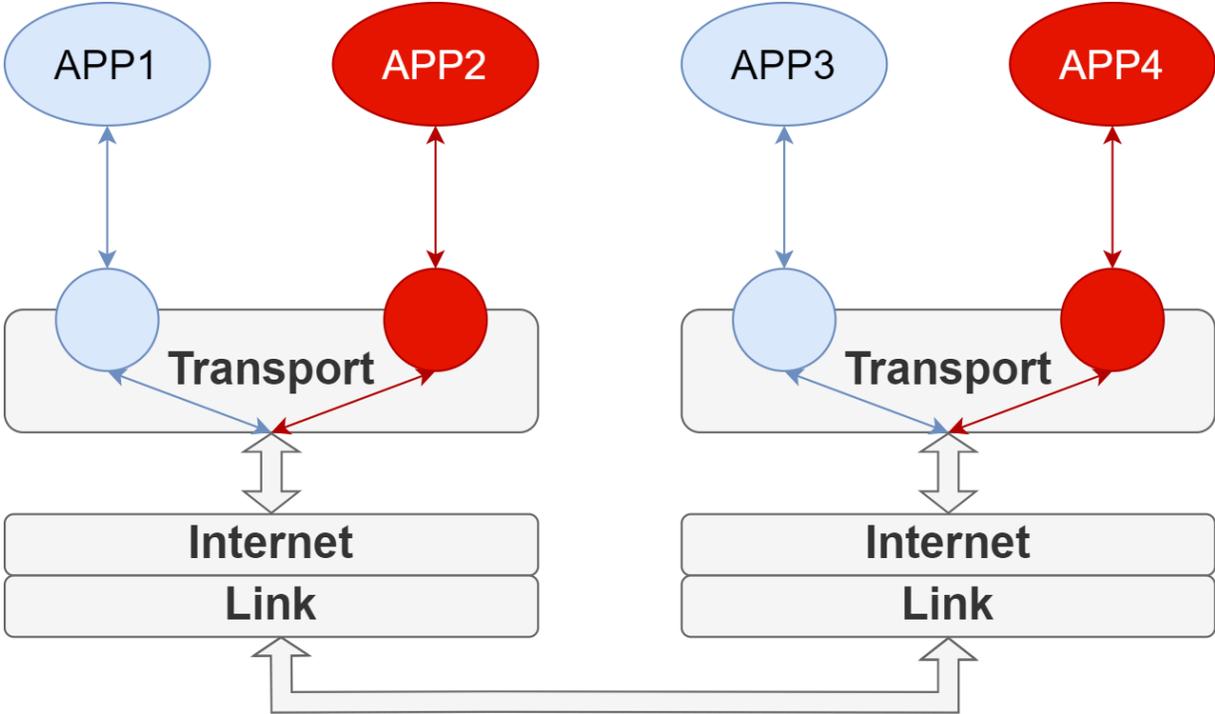
# TCP

## Задачи TCP



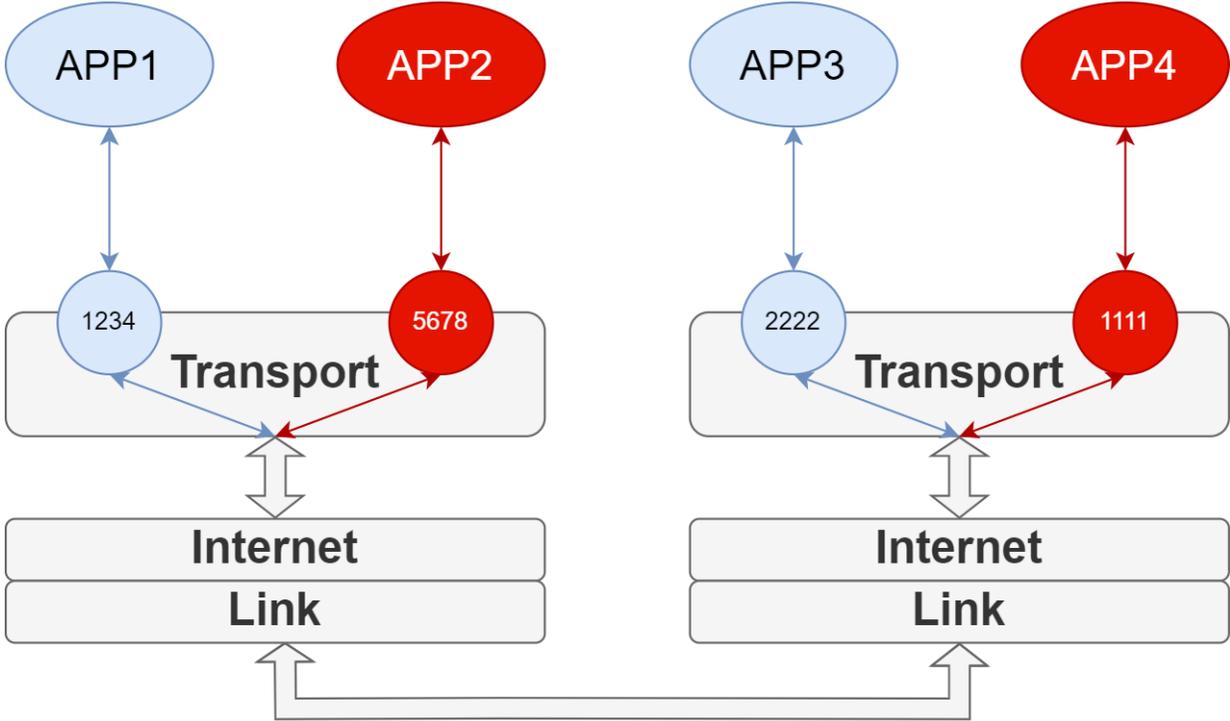
# Мультиплексирование сессий

Посредством мультиплексирования узел может поддерживать множество сессий и управлять отдельными потоками через единый канал



# Идентификация приложений

Для идентификации приложения используется число - порт  
 Порт приложения может быть фиксированным или произвольным  
 Порты TCP и UDP независимы



# Диапазоны портов

Хорошо известные (well-known) – с 1 по 1023

Зарегистрированные (registered) – с 1024 по 49151

Динамические, частные или эфемерные (dynamic, private или ephemeral) – с 49152 по 65535

# Терминология

## Сегментирование –

процесс разделения произвольного объема данных на части

Размер части должен быть таков, чтобы не был превышен MTU на сетевом уровне



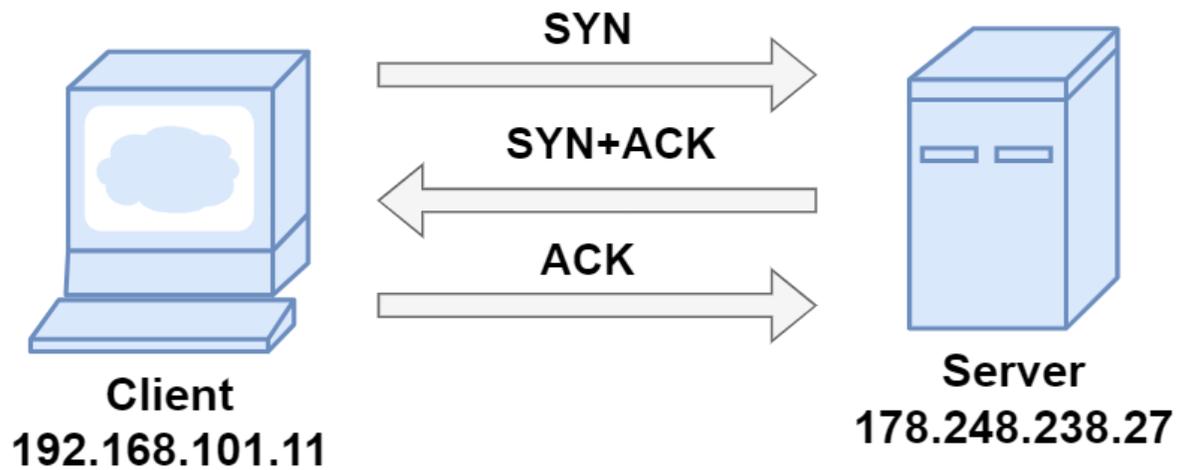
# Управление потоком

- Регулирует отправку сообщений таким образом, чтобы обеспечить максимальную скорость отправки и минимизировать повторную передачу сообщений
- Основной механизм управления потоком – подтверждения о получении данных
- Для повышения эффективности используется механизм скользящего окна

# Управление соединениями

- Перед отправкой данных по протоколу TCP узлы устанавливают соединение
- Узлы поддерживают соединение в течение всего сеанса передачи данных
- За счет отслеживания данных в соединении обеспечивается надежность
- Приложение, которое инициирует соединение называется клиент
- Приложение, которое ожидает соединение - сервер

# Установка соединения TCP

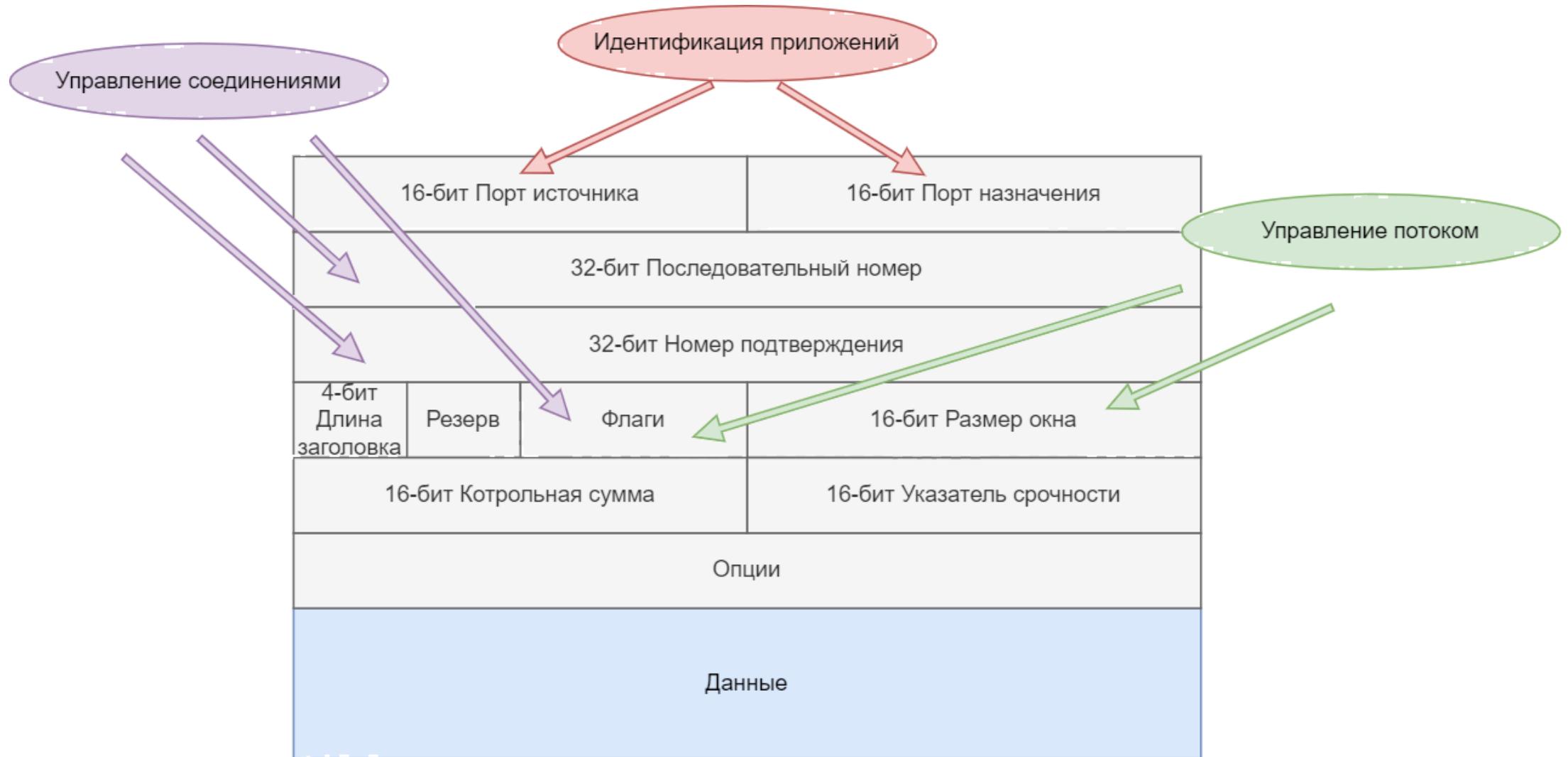


Source	Destination	Protocol	Info
192.168.101.11	178.248.238.27	TCP	52652 → 80 [SYN] Seq=0 Win=64240
178.248.238.27	192.168.101.11	TCP	80 → 52652 [SYN, ACK] Seq=0 Ack=1
192.168.101.11	178.248.238.27	TCP	52652 → 80 [ACK] Seq=1 Ack=1 Win=0

# Обеспечение надежности

- Обнаружение и повторная отправка потерянных сегментов
- Обнаружение и устранение повторов или неправильного порядка следования данных
- Предотвращение заторов в сети

# Задачи TCP



# UDP



## Заголовок UDP

16-бит Порт источника	16-бит Порт назначения
16-бит Длина UDP	16-бит Контрольная сумма
Данные	

# Сравнение TCP и UDP

TCP	UDP
Надежный	Быстрый
Устанавливает соединение	Отправка данных без соединения
Работает в режиме точка-точка	Может отправлять данные на несколько узлов

# Протокол ARP (Address Resolution Protocol)

- Используется для определения MAC адреса устройства
- Полученный, в результате работы протокола, MAC адрес помещается в ARP таблицу (кэш)

# Принцип работы ARP

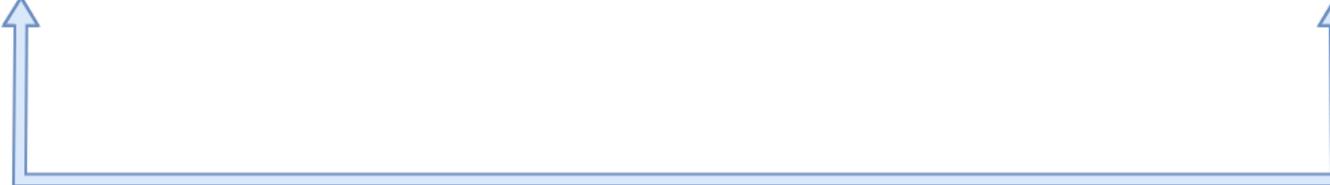
- Предположим, что узлу А необходимо отправить IP пакет узлу В
- Узел А «знает» IP адрес узла В, но не «знает» его MAC адрес

s=10.0.0.1 d=10.0.0.2 DATA

Host A  
IP=10.0.0.1  
MAC=0800.02aa.aaa



Host B  
IP=10.0.0.2  
MAC=0800.02bb.bbbb



# Принцип работы ARP

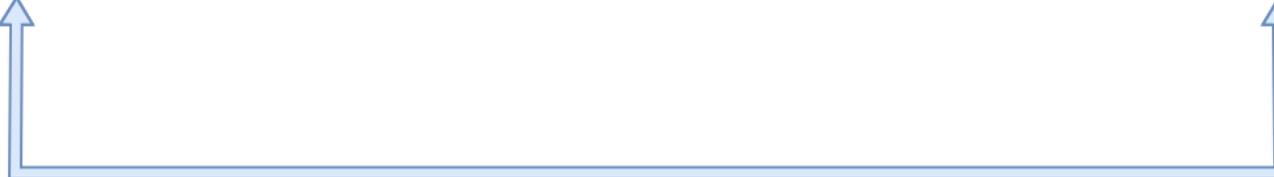
- Узел A определяет, что IP адрес узла B находится в той же подсети что и он сам
- Узел A проверяет локальную ARP таблицу
- Если в локальной ARP таблице соответствия нет, то формируется ARP запрос для определения MAC узла B

s=10.0.0.1 d=10.0.0.2 DATA

Host A  
IP=10.0.0.1  
MAC=0800.02aa.aaa



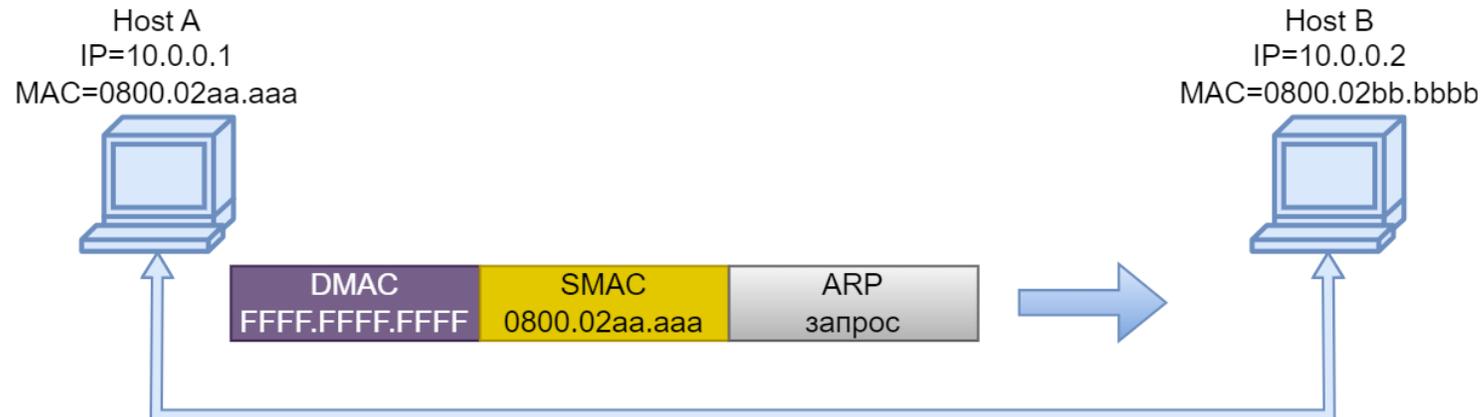
Host B  
IP=10.0.0.2  
MAC=0800.02bb.bbbb



# Принцип работы ARP

- Узел А отправляет широковещательный ARP запрос
- Все узлы в локальной сети его принимают и обрабатывают, в т.ч. и узел В
- Каждый узел сравнивает IP адрес в запросе со своим адресом
- Узел В определяет, что запрос адресован ему, поэтому добавляет в свою ARP таблицу соответствие IP и MAC адреса узла А

s=10.0.0.1 d=10.0.0.2 DATA



# Принцип работы ARP

- Узел В отправляет адресованный на MAC адрес узла А ARP ответ
- Только узел А его обрабатывает и добавляет в свою ARP таблицу соответствие IP и MAC адреса узла В

s=10.0.0.1 d=10.0.0.2 DATA

Host A  
IP=10.0.0.1  
MAC=0800.02aa.aaa



Host B  
IP=10.0.0.2  
MAC=0800.02bb.bbbb

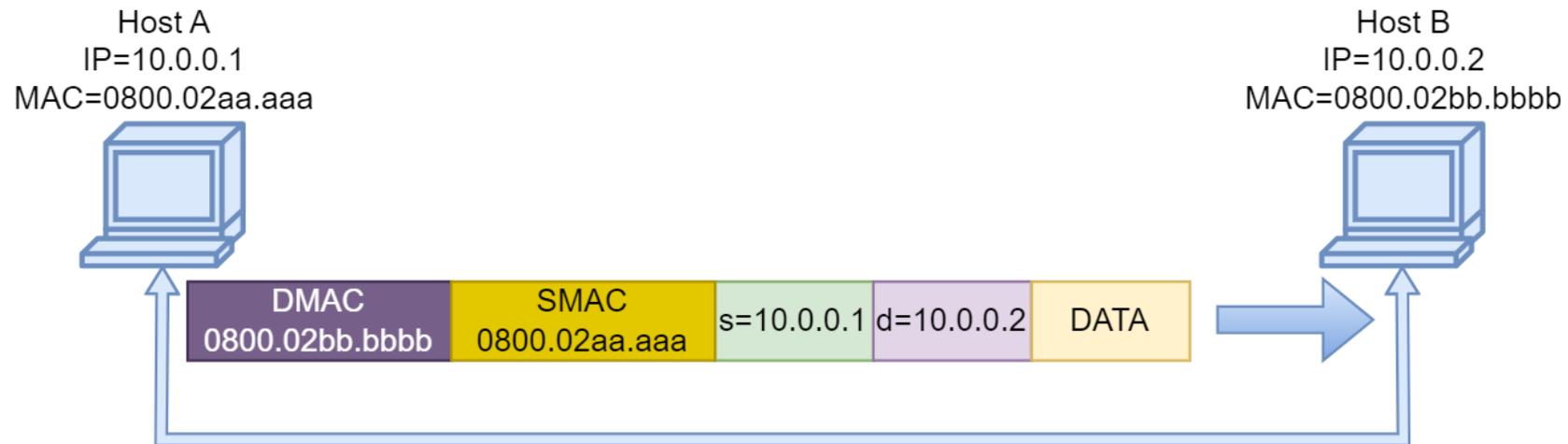


DMAC 0800.02aa.aaa    SMAC 0800.02bb.bbbb    ARP ответ



# Принцип работы ARP

- Выяснив MAC адрес узла B узел A формирует кадр с вложенным IP пакетом и отправляет его в сеть



# Содержимое ARP запроса и ответа

- В запросе содержится MAC адрес запрашивающего узла и IP адреса обоих узлов
- В ответе содержатся MAC и IP адреса обоих узлов



# ICMP

Протокол ICMP используется для:

- диагностики
- сообщения об ошибках
- автоконфигурации узлов (IPv6)
- обнаружение соседей (IPv6)

ICMP не исправляет ошибки передачи

# ICMP

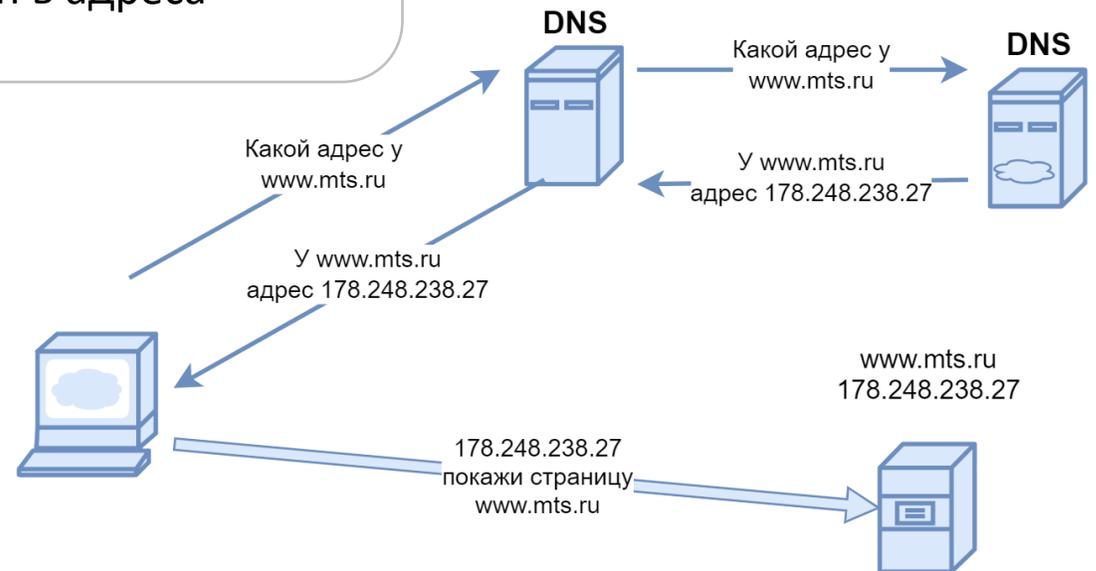
Каждое сообщение ICMP содержит три элемента:

- тип
- код
- данные (не обязательно)



# Система доменных имен (DNS)

- Адреса (набор цифр) не несут смысловой нагрузки для человека
- Имена более удобный способ идентификации компьютеров
- Система доменных имен – распределенная иерархическая база данных соответствия имен и адресов
- При настройке сетевых параметров требуется указать, какой сервер будет предоставлять услугу разрешения имен в адреса



# Демонстрация – настройка сети в Windows и Linux

- Настройка сети в Windows
- Настройка сети в Linux средствами графического интерфейса
- Настройка сети в Linux средствами командной строки

# Что мы изучили?

4. Основные протоколы TCP/IP

М

Т

Спасибо за  
внимание!

С