

# Обзор стека TCP/IP

# План

- ▶ Архитектура TCP/IP
- ▶ Поток данных по стеку
- ▶ Адресация на разных уровнях
- ▶ Установление соединения
- ▶ Протокол IPv4
- ▶ Протокол IPv6



# Архитектура и общая характеристика стека

# Стек TCP/IP

Стек TCP/IP - это набор иерархически упорядоченных сетевых протоколов.

Название стек получил по двум важнейшим протоколам:

- ▶ TCP (Transmission Control Protocol);
- ▶ IP (Internet Protocol).

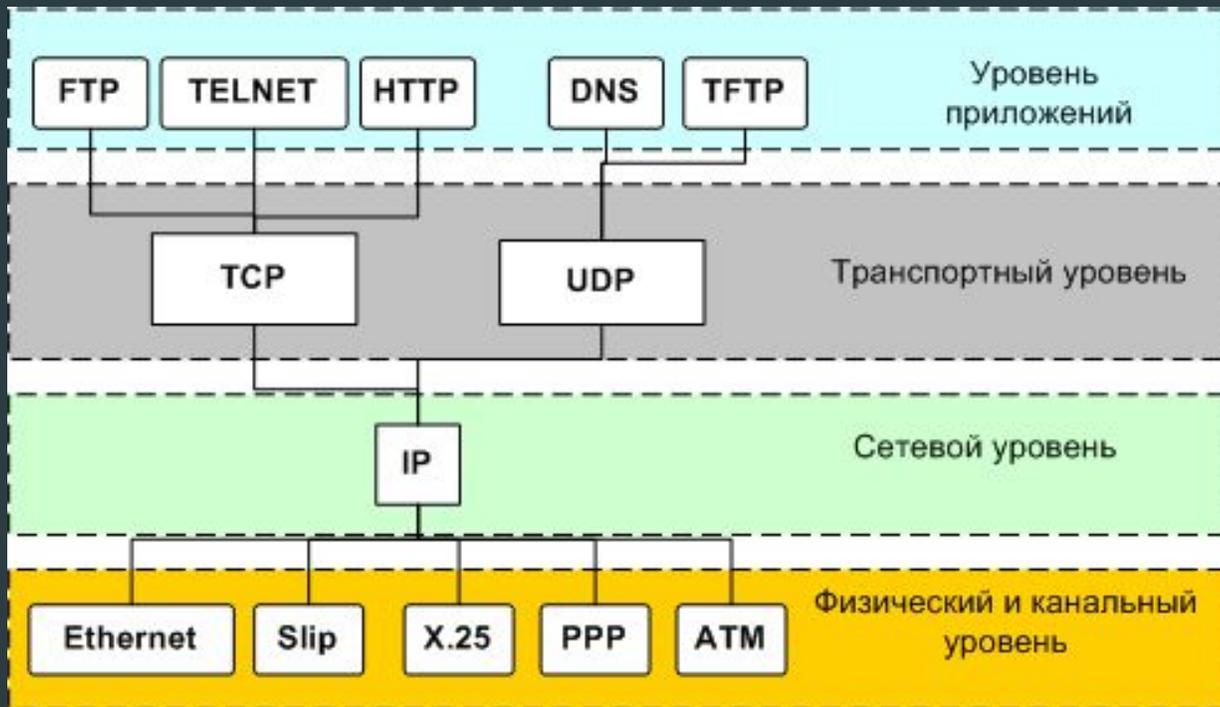
Стек протоколов TCP/IP обладает двумя важными свойствами:

- ▶ платформонезависимость;
- ▶ открытость.

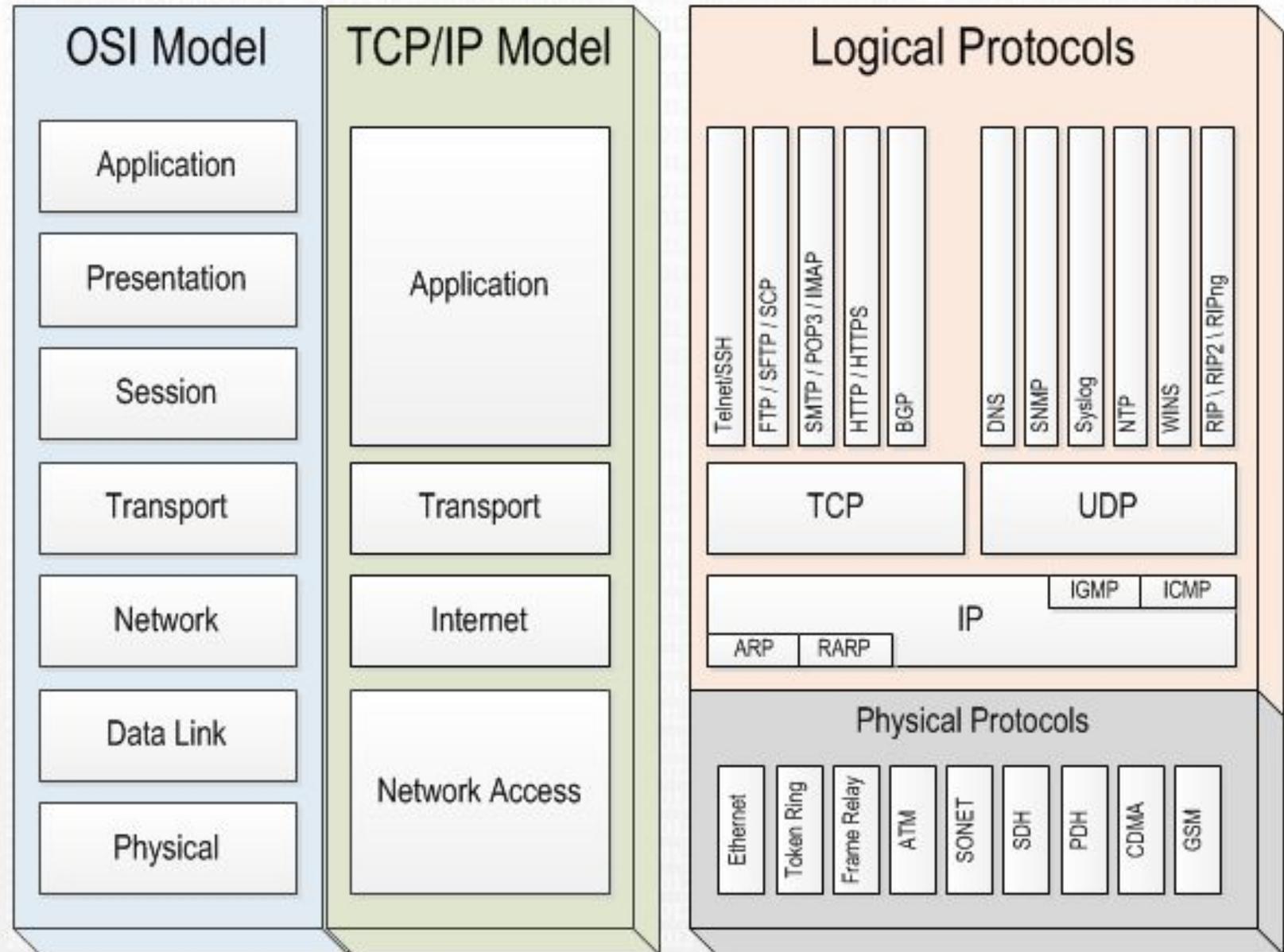
# История создания

- ▶ В 1967 году Агентство по перспективным исследовательским проектам министерства обороны США (ARPA - Advanced Research Projects Agency) инициировало разработку компьютерной сети, связывающей ряд университетов и научно-исследовательских центров, выполнявших заказы Агентства (ARPANET - в 1972 году соединяла 30 узлов).
- ▶ В рамках проекта ARPANET были разработаны и в 1980-1981 годах опубликованы основные протоколы стека TCP/IP - IP, TCP и UDP. (Модель OSI утверждена в 1984).
- ▶ 1 января 1983 года ARPANET перешла на новый протокол. 
- ▶ Важным фактором распространения TCP/IP стала его реализация в операционной системе UNIX 4.2 BSD (1983) университетом Беркли.
- ▶ К концу 80-х годов ARPANET стала называться Интернет (Interconnected networks - связанные сети) и объединяла университеты и научные центры США, Канады и Европы.
- ▶ 1992. Появление новый сервис Интернет - WWW (World Wide Web - всемирная паутина), основанный на протоколе HTTP.

# Стек TCP/IP



# TCP/IP и OSI



# Протоколы стека TCP/IP

Уровень приложений	FTP SMTP POP3 IMAP4 HTTP RDP SSH Telnet DNS LDAP			
Транспортный уровень	TCP		UDP	XTP
Межсетевой уровень	ICMP ARP RARP		IP	DHCP BOOTP ESP AH RIP OSPF BGP EGP
Уровень сетевого интерфейса	PPTP L2F SLIP		Интерфейсы к Ethernet, ATM, FDDI, WiFi И т.д.	

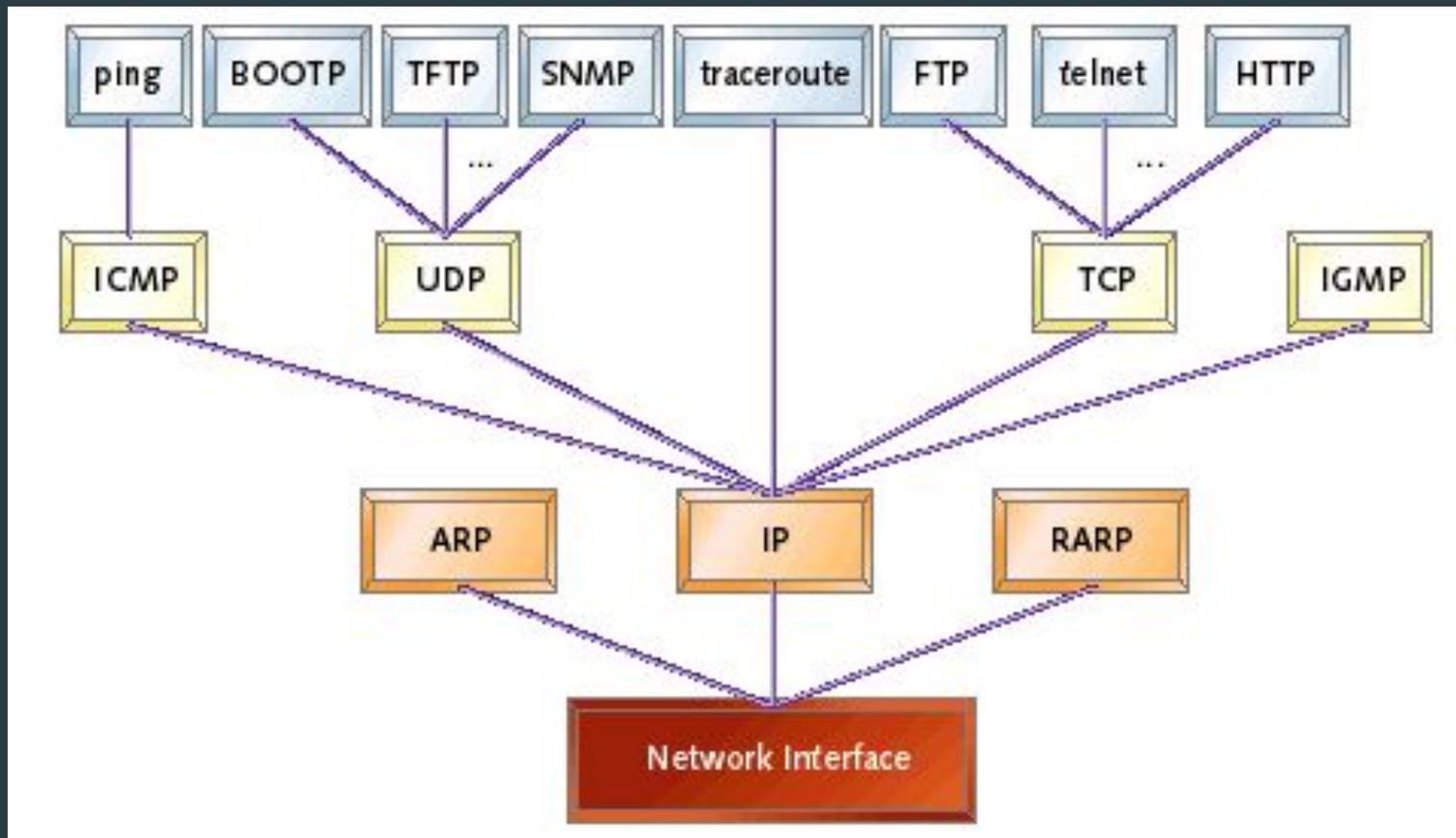
# Описание некоторых протоколов

- ▶ FTP (англ. File Transfer Protocol — протокол передачи файлов) - работает по протоколу TCP, порты 20 и 21. Предназначен для передачи файлов между сервером и клиентом. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.
- ▶ SMTP (англ. Simple Mail Transfer Protocol — простой протокол передачи почты) - работает по 25 порту TCP, предназначен для передачи сообщений электронной почты между клиентским программным обеспечением и сервером, а также между серверами. Не содержит стандартных средств авторизации отправителя (кроме расширений ESMTP для авторизации клиента).
- ▶ POP3 (англ. Post Office Protocol Version 3 - протокол почтового отделения, версия 3) - работает по 110 порту TCP. Предназначен для получения клиентом почтовых сообщений с сервера. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.
- ▶ HTTP (сокр. от англ. HyperText Transfer Protocol — протокол передачи гипертекста). Работает по портам 80, 8080 TCP. Предназначен для передачи текстовых и мультимедийных данных от сервера к клиенту по запросу последнего. В настоящее время используется как транспорт для других протоколов прикладного уровня.
- ▶ SSH (англ. Secure SHell — «безопасная оболочка») — сетевой протокол сеансового уровня
- ▶ Telnet (англ. TErминаL NETwork — протокол терминального сетевого доступа). Работает по 21 порту TCP. Предназначен для организации полнодуплексного сетевого терминала между клиентом и сервером. Команды выполняются на стороне сервера. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.
- ▶ DNS (англ. Domain Name System — система доменных имён). Работает по портам 53 UDP для взаимодействия клиента и сервера и 53 TCP для AFXR запросов, поддерживающих обмен между серверами. DNS - протокол поддерживающий работу одноименной распределённой системы, осуществляющей отображение множества доменных имен и множества IP адресов хостов.
- ▶ TCP (анг. Transmission Control Protocol - протокол управления передачей). Протокол транспортного уровня, обеспечивающий установку двунаправленного соединения между процессами, идентифицирующимися по сокету (комбинации IP адреса и порта), передачу потока сегментов внутри соединения с подтверждением приема, управление и завершение соединения. Сообщение TCP содержит в заголовке адреса сегментов в направленном потоке и контрольную сумму при расчете которой используется поле данных и заголовок. Для оптимизации передачи и предотвращения перегрузок сети используется механизм переменного окна, позволяющий вести передачу без получения подтверждения приема каждого сообщения. В качестве адресной информации использует порт.
- ▶ UDP (англ. User Datagram Protocol — протокол пользовательских дейтаграмм). Протокол транспортного уровня, обеспечивающий передачу сообщений между процессами, идентифицирующимися по сокету (комбинации IP адреса и порта). Сеанс не устанавливается, подтверждения приема не осуществляется. В качестве адресной информации использует порт.

# Поток данных по стеку



# Поток данных по стеку



# Надежная и ненадежная доставка

- ▶ Дейтаграммная передача
  - ▶ IP, UDP
- ▶ Передача с установкой соединений
  - ▶ TCP
  - ▶ QUIC + UDP

# RFC (Request for Comments)

- ▶ RFC - документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты
- ▶ Публикацией документов RFC занимается IETF под эгидой открытой организации Общество Интернета (англ. Internet Society, ISOC). Правами на RFC обладает именно Общество Интернета.
- ▶ Очерк истории RFC за 50 лет с 1969 по 2019 гг. представлен в RFC 8700
- ▶ <https://www.rfc-editor.org/retrieve/>



Адресная информация и  
установление соединения

# Адресация на разных уровнях

Уровень стека	Адрес	Пример
Прикладной уровень	DNS, X.500, WINS условно	www.ifmo.ru
Транспортный уровень	Номер порта TCP или UDP	443
Сетевой уровень	Ip адрес	192.168.0.103 fe80::59e1:d46b:1bb:5169
Канальный уровень	Media Access Control (MAC)	BC:EE:7B:5B:E5:E5

Синтетические адреса: URL, socket (ip:port)

# Установка соединения

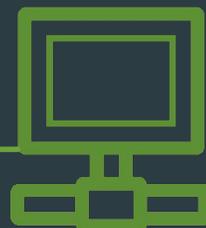
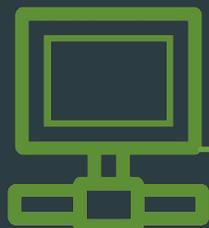
- ▶ Цель установить соединение между программой-клиентом и программой-сервером.
- ▶ Первичная конфигурация:
  - ▶ Назначаем IP адреса для компьютеров (предполагаем что маршрутизация работает)
  - ▶ Программа сервер при запуске занимает порт (пусть TCP). Номер порта известен заранее.
  - ▶ Программа клиент при запуске занимает свободный порт выше 1024.

Web-browser  
TCP 29384



Web-server  
TCP 80

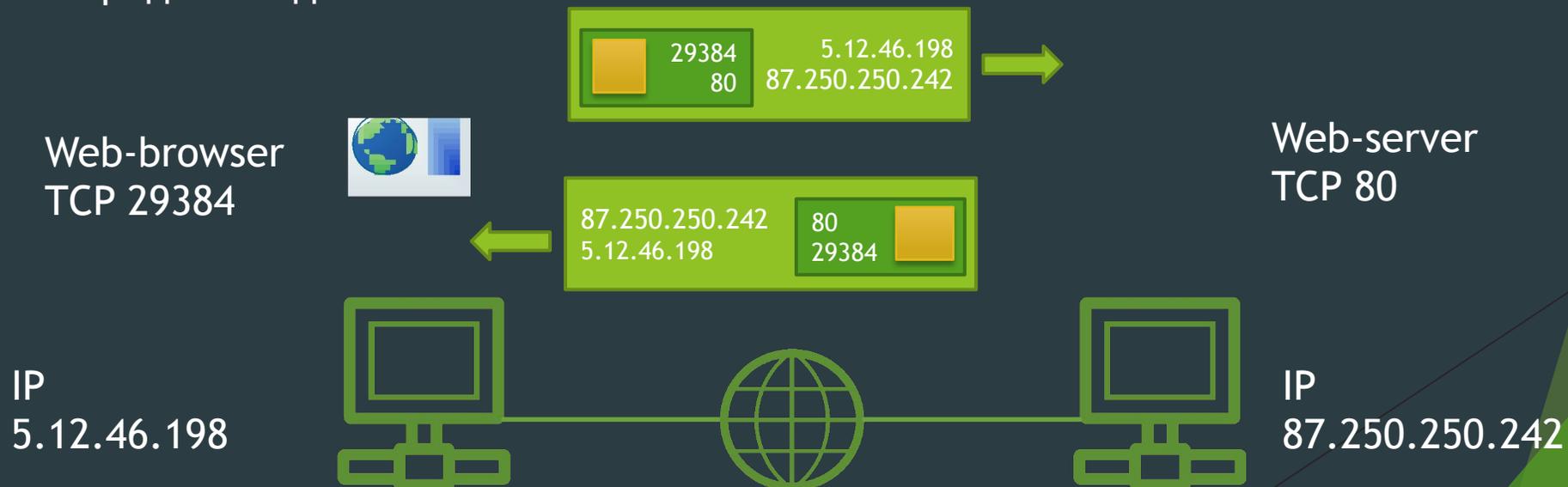
IP  
5.12.46.198



IP  
87.250.250.242

# Установление соединения

- ▶ Программа клиент передает модулям TCP и IP информацию о номере порта и адресе назначения.
- ▶ Передаются данные первого пакета (указывается номер порта отправителя и адрес отправителя).
- ▶ Целевой компьютер получает информацию и отвечает на запрос.
- ▶ Устанавливается соединение
- ▶ Передаются данные.



# Установление соединения

- ▶ У клиента случайный порт, а у сервера заранее известный.
- ▶ Соединение устанавливается со стороны клиента.
- ▶ Соединение идентифицируется двумя сокетами.



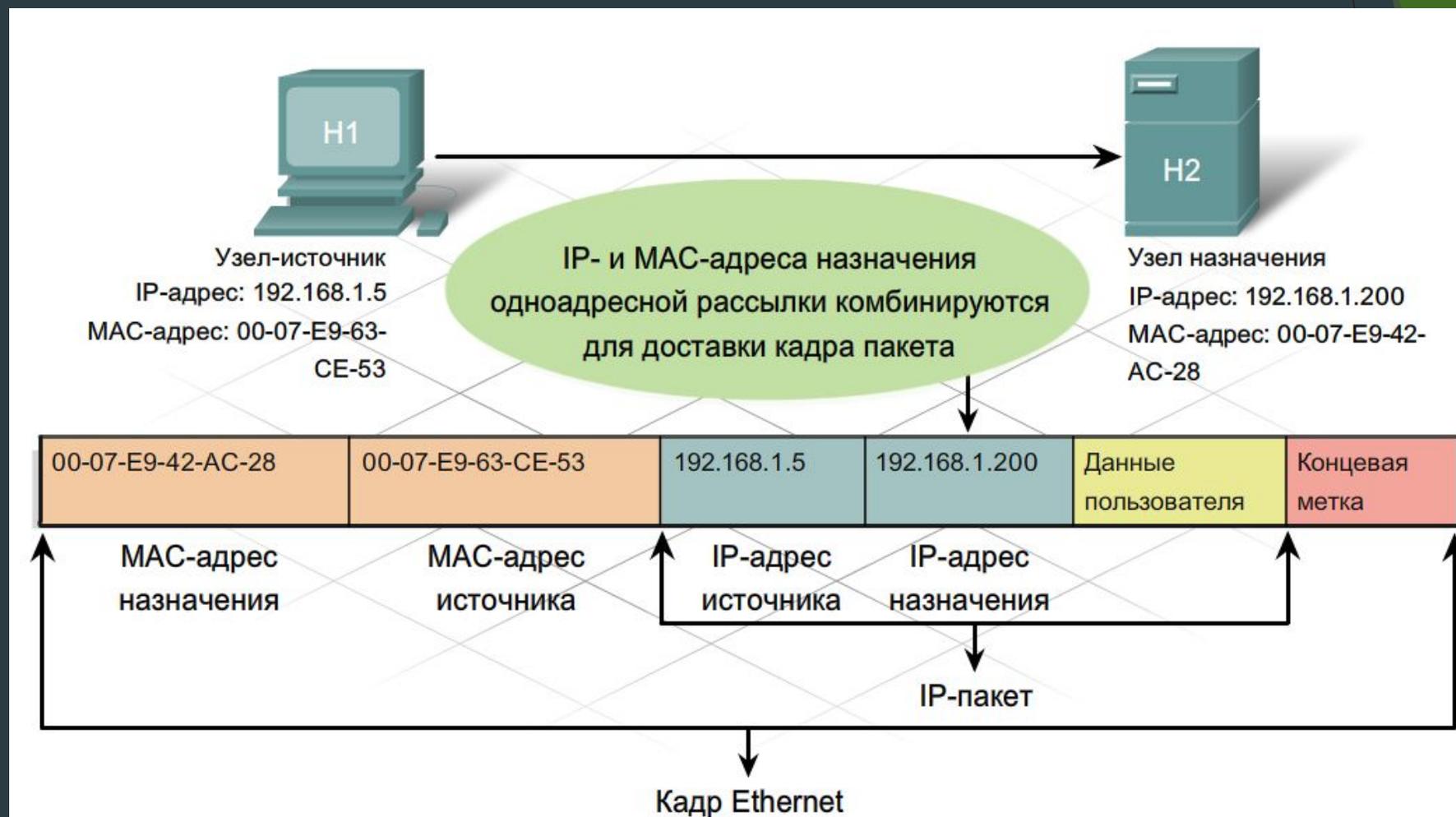
# Типы рассылок IP

# Типы рассылок

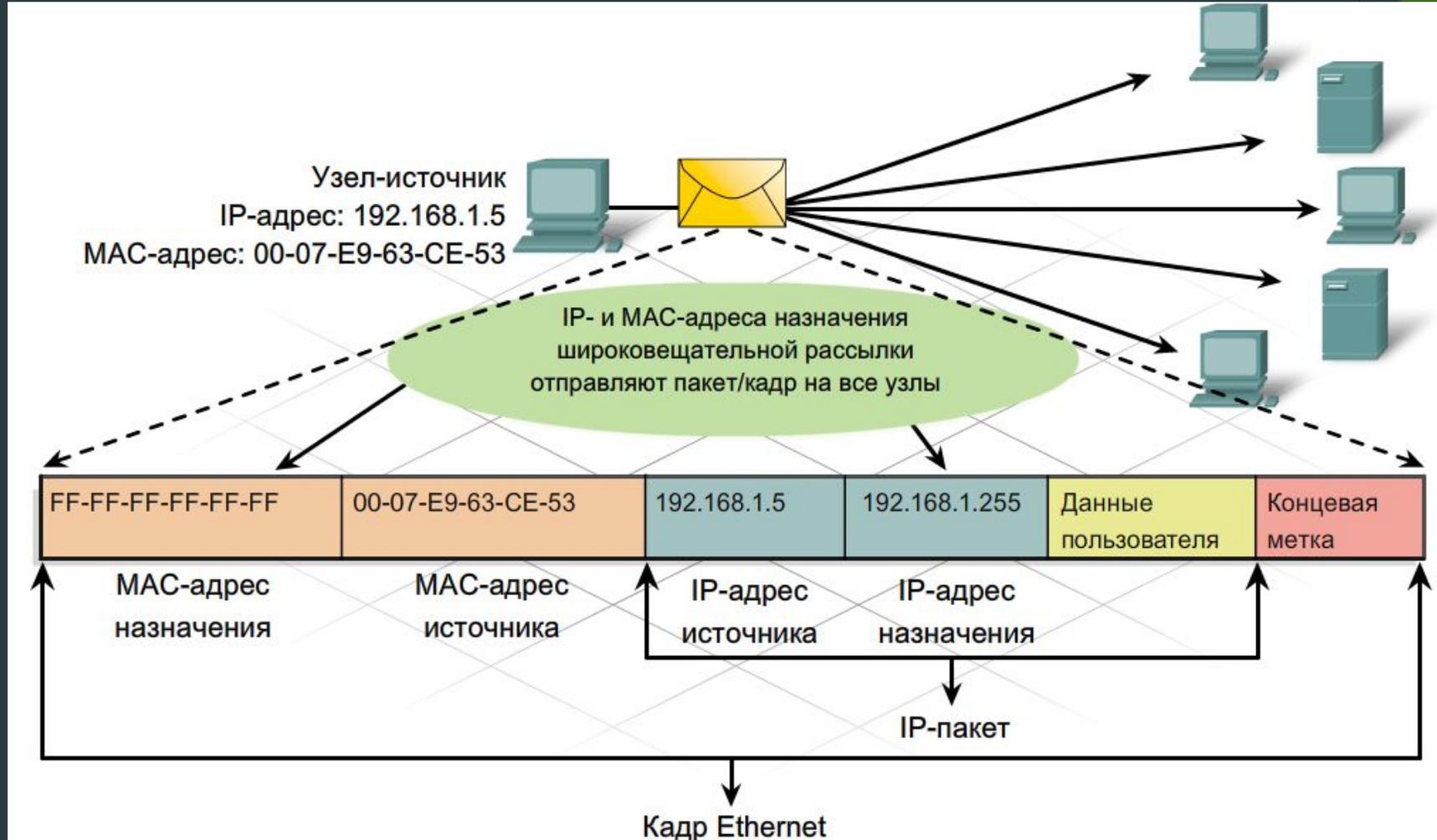
Помимо классов, IP-адреса делятся на категории, предназначенные для разных типов рассылок:

- ▶ «один к одному» (одноадресная рассылка);
- ▶ «один ко многим» (многоадресная рассылка);
- ▶ «один ко всем» (широковещательная рассылка).

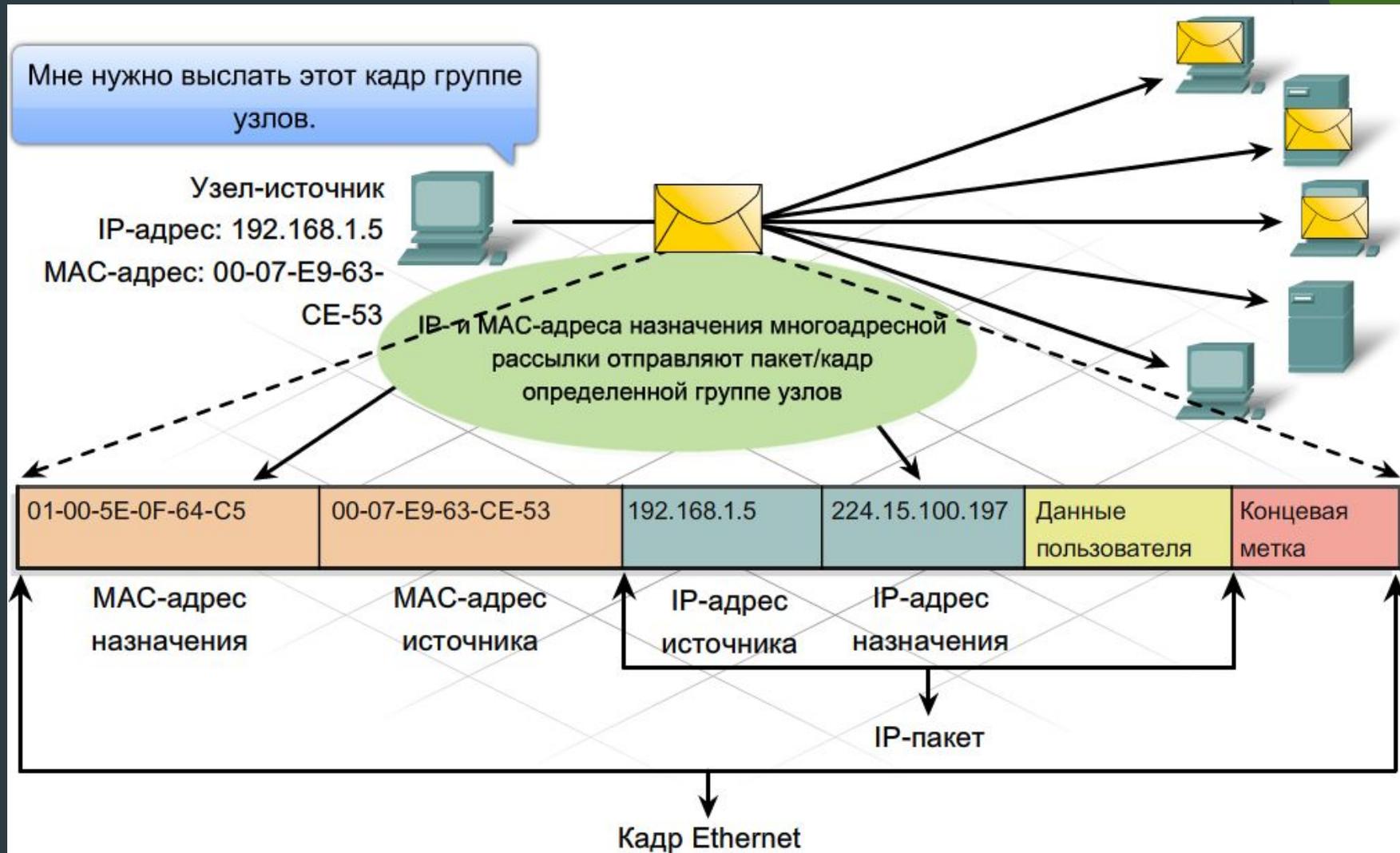
# Одноадресная рассылка



# Широковещательная рассылка



# Многоадресная рассылка





Адресация IP

# IP - адресация

IP-адрес - это уникальный числовой адрес, который однозначно идентифицирует узел, группу узлов или сеть.

IPv4-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел «октетов», разделенных точками - W.X.Y.Z Каждый октет может принимать значения в диапазоне от 0 до 255.

В протоколе IPv6 размер адреса составляет 128 бит. Предпочтительным является следующее представление адреса IPv6: x:x:x:x:x:x:x, где каждая буква x - это шестнадцатеричные значения шести 16-битных элементов адреса.

# Классовая и бесклассовая адресация

- ▶ Классовая IP адресация — это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т.к. не возможно использование различных масок подсетей. В классовой метод адресации используется фиксированная маска подсети, поэтому класс сети всегда можно идентифицировать по первым битам. *Не актуален.*
- ▶ Бесклассовая IP адресация (*Classless Inter-Domain Routing — CIDR*) — это метод IP-адресации, который позволяет рационально управлять пространством IP адресов. В бесклассовом методе адресации используются маски подсети переменной длины (*variable length subnet mask — VLSM*). *Пока актуален.*

# Деление адреса в IPv4

- ▶ Адреса делятся двумя способами:
  - ▶ классовая адресация
  - ▶ Бесклассовая адресация (с помощью масок)

# Классы IP-адресов

Классы IP-адресов					
Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зеленые биты не меняются)	Сетевая (С) и узловая (У) части адреса	Маска подсети по умолчанию (в десятичном и двоичном формате)	Число возможных сетей и узлов для каждой сети
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 сетей ( $2^7-2$ ) 16 777 214 узлов для каждой сети ( $2^{24}-2$ )
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 сетей ( $2^{14}-2$ ) 65 534 узла для каждой сети ( $2^{16}-2$ )
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 сетей ( $2^{21}-2$ ) 254 узла для каждой сети ( $2^8-2$ )
D	224 - 239	11100000 - 11101111	В качестве узла не для коммерческого использования		
E	240 - 255	11110000 - 11111111	В качестве узла не для коммерческого использования		

# Бесклассовая адресация

IP-адрес

Адрес сети

Адрес узла внутри сети

Маска

1111.....11111

0000...000

Запись:

192.168.0.200 mask 255.255.255.0

или

192.168.0.200/24

# Бесклассовая адресация

## Зачем знать маску при установке адреса?

- ▶ Для определения границ адресов LAN
- ▶ Для формальной проверки gateway
- ▶ Для организации широковещания



# Деление с помощью маски

- ▶ Пример 1 (192.168.0.0 mask 255.255.255.0 или 192.168.0.0/24)

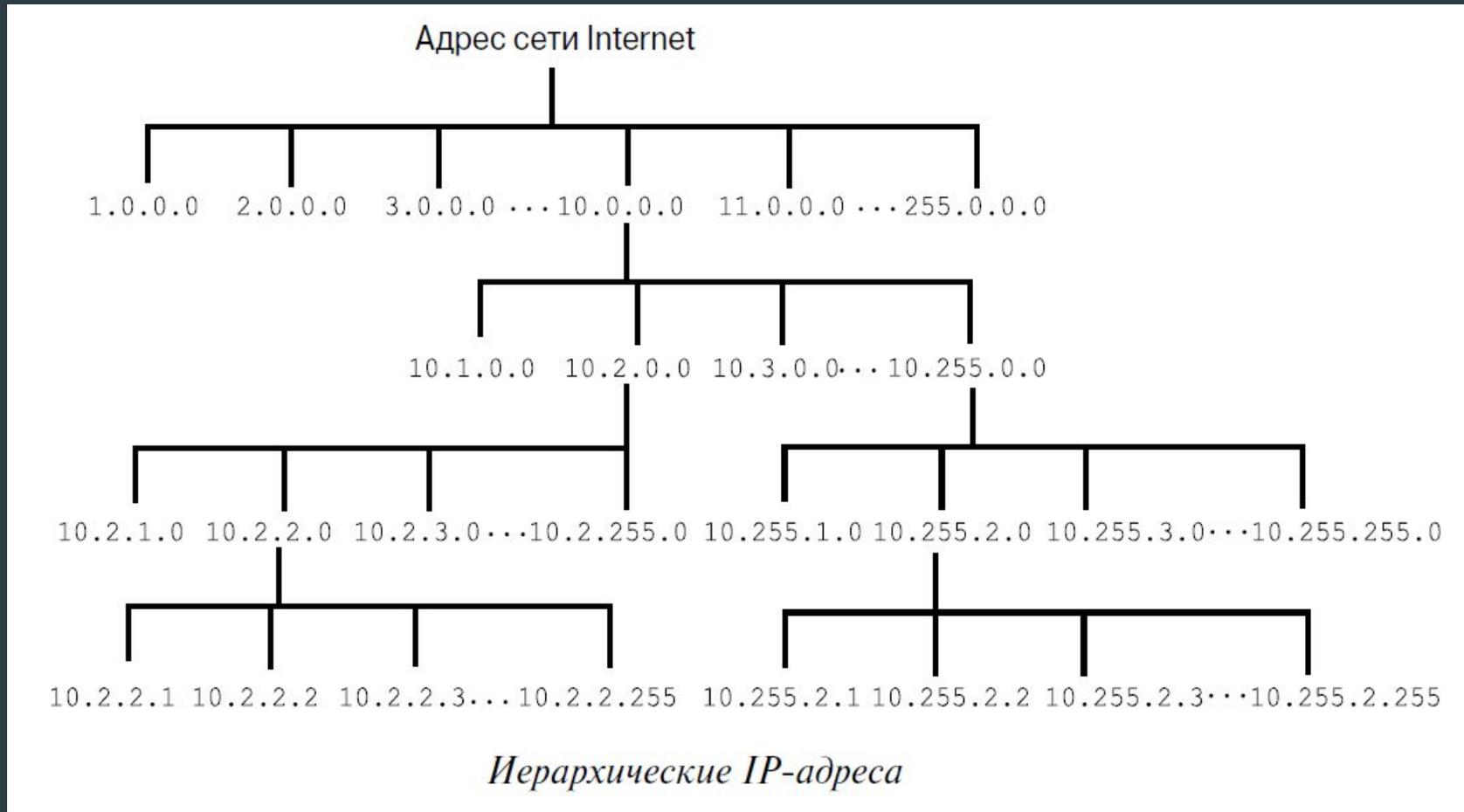
Имя	Значение	Бинарное значение
Адрес	192.168.0.1	11000000.10101000.00000000   00000001
<u>Bitmask</u>	24	
<u>Netmask</u>	255.255.255.0	11111111.11111111.11111111   00000000
<u>Network</u>	192.168.0.0	11000000.10101000.00000000   00000000
<u>Broadcast</u>	192.168.0.255	11000000.10101000.00000000   11111111
<u>Hostmin</u>	192.168.0.1	11000000.10101000.00000000   00000001
<u>Hostmax</u>	192.168.0.254	11000000.10101000.00000000   11111110
<u>Hosts</u>	254	

# Деление с помощью маски

- ▶ Пример 2 (192.168.0.0 mask 255.255.255.252 или 192.168.0.0/30)

Имя	Значение	Бинарное значение
Адрес	192.168.0.1	11000000.10101000.00000000.00000000   01
<u>Bitmask</u>	30	
<u>Netmask</u>	255.255.255.252	11111111.11111111.11111111.11111111   00
<u>Wildcard</u>	0.0.0.3	00000000.00000000.00000000.00000000   11
<u>Network</u>	192.168.0.0	11000000.10101000.00000000.00000000   00
<u>Broadcast</u>	192.168.0.3	11000000.10101000.00000000.00000000   11
<u>Hostmin</u>	192.168.0.1	11000000.10101000.00000000.00000000   01
<u>Hostmax</u>	192.168.0.2	11000000.10101000.00000000.00000000   10
<u>Hosts</u>	2	

# Иерархическая адресация



# Публичные и частные IP-адреса

В соответствии со стандартом RFC 1918 было зарезервировано несколько диапазонов адресов класса А, В и С.

Класс адреса	Число зарезервированных сетевых адресов	Сетевые адреса
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

# Специальные IP адреса

- ▶ 127.0.0.0 / 8
- ▶ Адрес сети
- ▶ Адрес широковещания
- ▶ Особые адреса назначения



Адресация IPv6

# Адреса IPv6

## ► Формат

В протоколе IPv6 размер адреса составляет 128 бит. Предпочтительным является следующее представление адреса IPv6: x:x:x:x:x:x:x:x, где каждая буква x - это шестнадцатиричные значения шести 16-битных элементов адреса.

Диапазон адресов IPv6 составляет от

0000:0000:0000:0000:0000:0000:0000:0000

до

ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

# Адреса IPv6

2001:0DB8:00AF:ABCD:0000:0000:0000:0034

▶ Правила сокращения при записи:

- ▶ Убираем ведущие нули:

2001:DB8:AF:ABCD:0000:0000:0000:34

- ▶ Убираем длинные последовательности нулей:

2001:DB8:AF:ABCD::34

# Типы адресов

- ▶ **Unicast** адреса идентифицируют только один сетевой интерфейс. Протокол IPv6 доставляет пакеты, отправленные на такой адрес, на конкретный интерфейс.
- ▶ **Anycast** адреса назначаются группе интерфейсов, обычно принадлежащих различным узлам. Пакет, отправленный на такой адрес, доставляется на один из интерфейсов данной группы, как правило наиболее близкий к отправителю с точки зрения протокола маршрутизации.
- ▶ **Multicast** адрес также используется группой узлов, но пакет, отправленный на такой адрес, будет доставлен каждому узлу в группе.
- ▶ Бродкаста нет

# Логические части адреса IPv6

Вместо масок сетей - префиксы от 0 до 128 (стандартно - 64)



# Префиксы адреса

Длина префикса кратна 16:

- Адрес: 2a02:06b8:0892:ad61:59a2:3149:c5a0:67a4/64
- Префикс: 2a02:06b8:0892:ad61:0000:0000:0000:0000

Длина префикса кратна 4:

- Адрес: 2a02:06b8:0892:ad61:59a2:3149:c5a0:67a4/52
- Префикс: 2a02:06b8:0892:a000:0000:0000:0000:0000

Длина префикса не кратна 4:

- Адрес: 2a02:6b8:0892:ad61:59a2:3149:c5a0:67a4/54
- Префикс: 2a02:6b8:0892:ac00:0000:0000:0000:0000

# Виды адресов

- ▶ **Global unicast адрес**

Аналог адреса белого адреса IPv4. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. Начинается с 2 или с 3. От 2000 до 3FFF. Из этой группы отдельно выделяется сеть 2001:0DB8::/32

- ▶ **Link-local**

Local IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу и только по данному каналу (подсети). Не является аналогом «серого» IPv4. Локальные IPv6-адреса канала находятся в диапазоне FE80::/10. /10

# Виды адресов

- ▶ **Loopback**  
Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 - `::1/128` или просто `::1`.
- ▶ **Unspecified address**  
Неопределённый адрес состоит из нулей и в сжатом формате представлен как `::/128` или просто `::`. Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес.

# Виды адресов

- ▶ **Unique local**

Unique local – IPv6-адреса имеют некоторые общие особенности с «серыми» адресами IPv4, но имеют и значительные отличия. Находятся в диапазоне от FC00::

- ▶ **IPv4 embedded**

Использование этих адресов способствует переходу с протокола IPv4 на IPv6.

- ▶ **Multicast**

Для рассылок внутри группы. Начинаются с FF.

# Структура адреса

## Global unicast адрес

Префикс глобальной маршрутизации	Ид. подсети	Идентификатор интерфейса
48 бит	16 бит	64 бита
Префикс сети		Идентификатор интерфейса

Префикс глобальной маршрутизации выдается IANA

Пример адреса: 2001:DB8:AF:ABCD::34

# Примеры структуры адреса

**2001:0DB8:0234:AB00:0123:4567:8901:ABCD**

**2** Global Unicast  
Address Indicator

**001** Region

**0DB8** Local Internet Registry (LIR)  
or Internet Service Provider (ISP)

**0234** Customer

**AB00** Subnet

**0123:4567:8901:ABCD**  
The 64-bit Extended Unique Identifier  
(EUI-64™)

# Структура адреса

## Unique local

FD	Префикс глобальной маршрутизации	Ид. подсети	Идентификатор интерфейса
8 бит	40 бит	16 бит	64 бита
Префикс сети			Идентификатор интерфейса

Определяется по RFC 4193

Пример адреса: fde8:86a5:fe80:1:5922:49:50:6767

# Структура адреса

## Link-local

Fe80	Ид. подсети	Идентификатор интерфейса
16 бит	48 бит	64 бита
Префикс сети		Идентификатор интерфейса

Пример адреса: fe80::59e1:d46b:1bb:5169

# Особые адреса

::/128 – текущий хост

::/0 – маршрут по умолчанию

::1/128 – обратная петля (loopback)

ff02::1 – все узлы в канале связи

ff02::2 – все маршрутизаторы в канале связи

# План

- ▶ Архитектура TCP/IP
- ▶ Поток данных по стеку
- ▶ Адресация на разных уровнях
- ▶ Установление соединения
- ▶ Протокол IPv4
- ▶ Протокол IPv6