

# Что такое IP-адрес.

Category: Справочная информация  
2026-10-12

## 1. Введение.

В мире доминируют сети с **IP-адресацией**, самая крупная из которых – **Интернет**. Устройства, начиная от bluetooth-гаджетов и заканчивая компьютерами, имеют собственный **IP-адрес**, который служит определяющей меткой в сетевом пространстве.

Понимание того, как работает **IP-адрес**, является основой системного администрирования. Это базовые знания, которые нужны в реальном мире для простейшей конфигурации сетей как в домашней, так и корпоративной среде.

В этой статье описывается простыми словами, что такое **IP-адрес**, какова его структура и предназначение, а также – как посмотреть **IP-адрес** несколькими способами. Затрагивается тема безопасности в **IP-сетях**, приводятся примеры основных угроз и способы защиты от них.

## 2. Что такое IP-адрес.

**IP-адрес** (**IP** от англ. **Internet Protocol**) – цифровой идентификатор, присваиваемый устройству, которое работает в условиях публичной или локальной сети на основе стека протоколов **TCP/IP**. Без него невозможно существование **Интернета** или какой-либо внутренней **IP-сети**.

Сравнить **IP-адрес** можно с номером телефона или адресом дома – и тот, и тот указывают на объект. Как человек звонит собеседнику по номеру, так и компьютер обращается к другому устройству по **IP-адресу**.

### 2.1. Структура IP-адреса.

Разберём структуру **IP-адреса** на примере самого первого и распространённого интернет-протокола **IPv4**.

# Структура IP-адреса

IPv4 в десятиричном виде



**IP-адрес** интернет-протокола **IPv4** имеет 32-битную (4 байта) структуру. Он разделён на 4 части, каждая из которых состоит из 8 бит (1 байт) и называется октетом. Каждый бит **IP-адреса** – цифра двоичной системы.

Пример адреса (**IPv4**) в двоичном виде:  
11000000.10101000.00110010.00000001.

При преобразовании октета с двоичной системы в десятиричную получается одно число со значением от 0 до 255.

**IP-адрес** в десятиричном виде: 192.168.50.1.

## 2.2. Маска подсети.

Устройства различают части **IP-адреса** при помощи маски подсети – 32-битной строки, разделённой на 4 октета, как и **IP-адрес**. При установке соединения каждый октет **IP-адреса** сопоставляется с октетом маски подсети.

По умолчанию в стандартной домашней сети маска подсети имеет вид: 255.255.255.0.

В примере маска **IP-адреса** указана в десятиричном представлении и содержит числа 255 и 0. Первое отвечает за **идентификацию сети**, а

второе за обозначение конечного узла.

## 2.3. Классы IP-адресов.

- **Класс А.** Старший бит в адресах такого формата всегда равен 0. За идентификацию сети отвечает начальный октет, позволяющий разместить 127 уникальных сетей. Оставшиеся 3 октета используются для обозначения узлов, максимальное количество которых составляет 17 млн на каждую сеть.
- **Класс В.** Первые биты **IP-адреса** равны 10. Начальные два октета относятся к идентификатору сети, а последние два – к идентификатору узла. Возможно создание 16384 сетей, каждая из которых поддерживает размещение 65000 узлов.
- **Класс С.** Начальные биты **IP-адреса** равны 110. За идентификацию сети отвечают первые три октета, позволяющие создать 2 млн сетей. Последний октет отводится для идентификации узлов, максимальное число которых составляет 254 на каждую сеть.
- **Класс D.** Запись **IP-адреса** начинается с битов 1110. В сетях подобного формата используется широковещательная рассылка сообщений нескольким узлам.
- **Класс Е.** Такие **IP-адреса** зарезервированы для использования в будущем. Первые биты всегда равны 11110.

**IP-адрес** в классовой архитектуре сетевой адресации состоит из двух частей:

- **Идентификатор сети.** Определяет сеть, содержащую подключённые узлы.
- **Идентификатор узла.** Отвечает за обозначение узла – сервера, маршрутизатора или любого другого **TCP/IP-устройства**.

**Важно!** В связи с ограниченностью ресурса адресов IPv4, в настоящее время классовая адресация почти перестала использоваться. Ей на смену пришла технология бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR). Бесклассовая адресация более экономно использует диапазон адресов IPv4, так как в ней нет строгой привязки масок подсети к адресам подсети.

## 2.4. Частные диапазоны IP-адресов.

**IPv4:**

- 10.0.0.0-10.255.255.255 – маска подсети для бесклассовой адресации: 255.0.0.0 или /8;
- 100.64.0.0-100.127.255.255 – маска подсети: 255.192.0.0 или /10;
- 172.16.0.0-172.31.255.255 – маска подсети: 255.240.0.0 или /12;

- 192.168.0.0-192.168.255.255 – маска подсети: 255.255.0.0 или /16.

#### IPv6:

- fc00::/7 – это 7-битный префикс адреса.

#### Петлевые интерфейсы:

- 127.0.0.0-127.255.255.255 – маска подсети: 255.0.0.0 или /8.

## 3. TCP/IP.

Любая сеть с **IP-адресацией** построена на основе **TCP/IP-модели**, включающей в себя стек протоколов, применяемых при передаче данных по сети. Основными протоколами являются **TCP** и **IP**, но имеется и масса других вариантов.

### 3.1. Уровни TCP/IP.

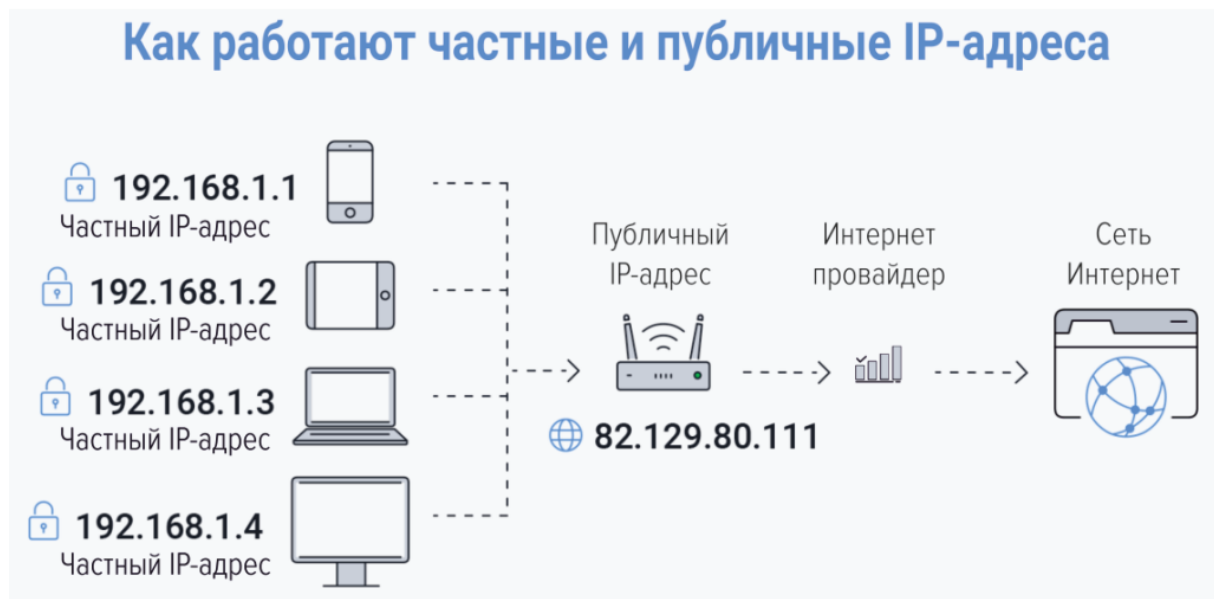


- **Канальный.** Отвечает за физическую передачу данных посредством использования таких протоколов, как **Ethernet** или **Wi-Fi**.
- **Сетевой (Интернет).** На этом уровне находится система **IP-адресов**, и осуществляется маршрутизация – перемещение пакетов между устройствами. Сетевой уровень совмещает протоколы: **IP**, **ICMP**, **IGMP**.
- **Транспортный.** Здесь расположены протоколы **TCP** и **UDP**, отвечающие за передачу данных. Первый осуществляет гарантированное

перемещение информации, предварительно устанавливая соединение с сетью. Второй же отправляет сообщения без осуществления «рукопожатия», что повышает скорость передачи данных, но также создаёт риск потери отдельных пакетов.

- **Прикладной.** Совмещает все высокоуровневые протоколы, взаимодействующие с системными приложениями. К таким относятся Telnet, FTP, SMTP, SNMP и подобные.

### 3.2. Сетевое расположение IP-адресов.



Уникальные **IP-адреса**, которые назначаются специальными организациями (например, Интернет-провайдером), называются **внешними, белыми** или **публичными**. **Публичные IP-адреса** применяются для получения доступа к **Интернету** и осуществления взаимодействия с другими узлами через публичную сеть. Устройство с внешним **IP-адресом** видно другим пользователям в **Интернете**.

Кроме того, существуют **частные IP-адреса**, именуемые также **серыми** или **внутренними**. **Серые IP-адреса** назначаются устройствам в локальной сети и не видны в **Интернете**. К примеру, можно представить дом, в котором к **Wi-Fi** роутеру подключено несколько устройств. Все они объединены в одну сеть и имеют серые **IP-адреса**.

| Публичные IP-адреса                                                          | Частные IP-адреса                                                                                    |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Глобальный (внешний) охват.                                                  | Местный (внутренний) охват.                                                                          |
| Используются для соединений через Интернет за пределами частной сети.        | Используется для связи с другими устройствами в частной сети.                                        |
| Уникальный числовой код, не используемый другими устройствами.               | Неуникальный числовой код, который может использоваться другими устройствами в других частных сетях. |
| Можно узнать по поисковому запросу типа: «Мой IP-адрес» («What is my IP»).   | Можно найти во внутренних настройках устройства.                                                     |
| Назначаются интернет-провайдером.                                            | Присваиваются маршрутизатором конкретному устройству.                                                |
| Платные.                                                                     | Бесплатные.                                                                                          |
| Может использоваться любое число, не входящее в диапазон частных IP-адресов. | 10.0.0.0 – 10.255.255.255<br>172.16.0.0 – 172.31.255.255<br>192.168.0.0 – 192.168.255.255            |
| Пример: 8.8.8.8.                                                             | Пример: 10.11.12.13                                                                                  |

### 3.3. Присвоение IP-адресов.

#### 3.3.1. Динамическое назначение.

При подключении к сети через **протокол динамической настройки узла (DHCP / Dynamic Host Configuration Protocol)** все параметры стека **ТСР/IP** автоматически устанавливаются на устройстве. Узлу назначается **динамический IP-адрес**, который меняется на другой при переподключении устройства. Диапазон **IP-адресов** указывается на сервере **DHCP**.

#### 3.3.2. Статическое назначение.

Статический **IP-адрес** присваивается вручную и не изменяется при переподключении к сети. Этот тип присваивания используется на устройствах, доступ к которым должен производиться по одному адресу (например, на серверах).

### 3.4. Версии IP.

#### 3.4.1. IPv4.

# Адрес Ipv4

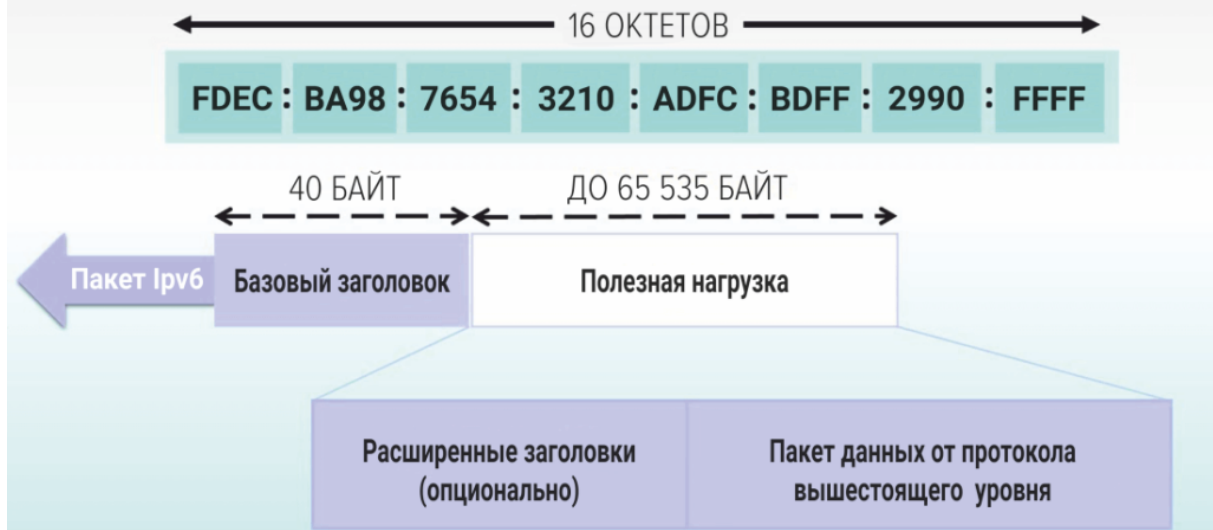


В сентябре 1981 года появился первый стандарт **интернет-протокола (IP) IPv4**, который положил начало современной сети **Интернет**.

**IPv4 IP-адрес** имеет вид: 192.168.50.1.

## 3.4.2. IPv6.

# Адрес Ipv6



Интернет с 1980-х годов начал стремительно расти, поэтому появилась угроза истощения пула возможных адресов – их просто не хватило бы на все сети и узлы. Поэтому в 1995 году появился формат **IPv6**, при котором длина **IP-адреса** возросла с 32 до 128 бит, а десятичная система сменилась шестнадцатеричной.

**IP-адрес** интернет-протокола **IPv6** состоит из 16 октетов (8 блоков по 2 октета), разделённых двоеточиями.

В полном виде запись **IPv6** выглядит следующим образом: 2001:0bd7:0ccf:0006:0000:0000:012f:002d.

Адрес **IPv6** можно сжать, исключив нули из записи.

Сокращенная форма **IPv6**: 2001:bd7:ccf:12f:2d.

### 3.4.3. Развитие IPv6.

Новый формат **IP-адреса** развивается сравнительно медленно. Первое внутреннее внедрение произошло у **Google** ещё в 2008, тогда протокол прошёл успешное тестирование. В прошлом 6 июня 2012 года совершился повсеместный запуск **IPv6**.

Число возможно доступных **IPv6** адресов равняется 340 ундециллионам (ундециллион – число с 36 нулями). Для сравнения, в формате **IPv4** этот показатель не превышает отметки 3,4 миллиона **IP-адресов**.

Многие провайдеры стали предоставлять пользователям услуги с использованием новой технологии. Основным фактором, замедляющим процесс внедрения **IPv6**, является необходимость замены оборудования провайдеров на более новое, что несёт дополнительные затраты.

## 4. DNS и IP-адрес.

Путешествуя по **Интернету**, пользователь устанавливает соединение через браузер с другими серверами в основном не по **IP-адресу**, а с помощью доменного имени. Система доменных имён (**DNS**) служит для перенаправления на постоянный **IP-адрес** конечного **web-ресурса**. Говоря простыми словами, она преобразовывает буквенные значения доменного имени в цифры **IP-адреса**.

Например, чтобы попасть на сайт поисковика **Google**, не нужно вводить сложный в запоминании числовой адрес 74.125.131.100. Достаточно набрать в адресной строке доменное имя .google.com.

За осуществление подобной переадресации отвечает **DNS-сервер**, который работает согласно информации из **DNS-записей**. Продолжая «телефонную» аналогию можно сказать, что если **IP-адрес** – это номер телефона, то сервер **DNS** – это телефонная книга, содержащая все подобные номера.

## 5. Как узнать IP-адрес.

Определить **IP-адрес** используемого устройства можно при помощи поискового запроса в браузере вида «мой ip-адрес» («What is my IP»). Многие сервисы проверяют идентификатор **IP-адреса** и предоставляют более подробную информацию о пользователе (например, название провайдера или примерное местоположение устройства).

В локальной сети адрес устройства указывается в настройках операционной системы, поэтому прибегать к внешним инструментам не требуется.

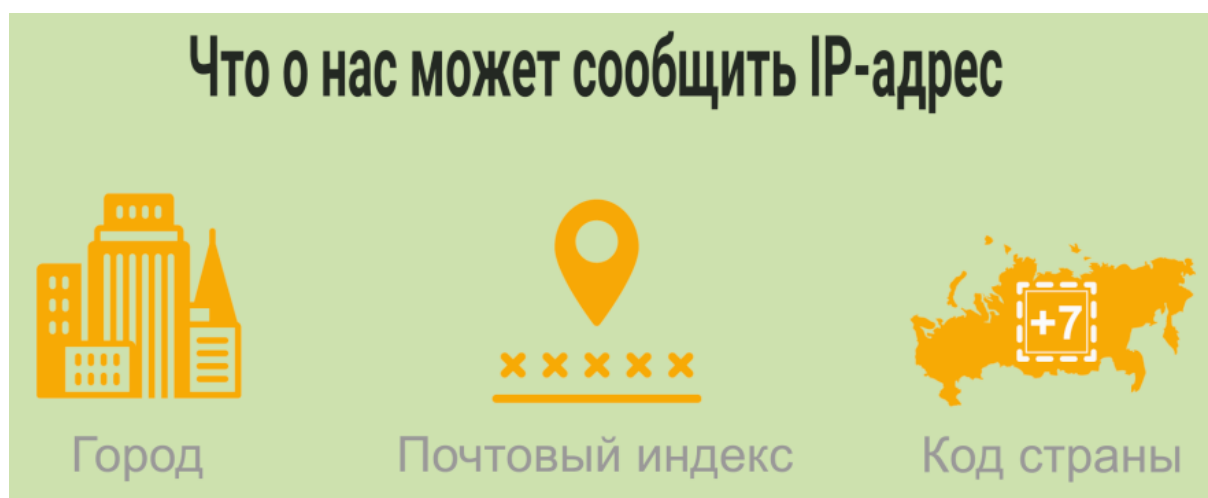
Определить **локальный IP-адрес** можно следующими способами.

- **Windows** – через командную строку (**Поиск** → «cmd» -> В окне прописать «ipconfig»).
- **GNU/Linux** – с помощью команды «ifconfig».
- **MacOS** – **Системные настройки** → **Сеть**.
- **iOS** – через **Настройки. Wi-Fi** → Нажать значок информации «i» -> Информация во вкладке **DHCP**.
- **Android** – **Настройки** → **0 телефоне** → **Общая информация**.

## 6. Анонимность и безопасность.

### 6.1. «Вычислю по IP».

Это скорее миф, чем реальная угроза. Среди пользователей существует заблуждение, что злоумышленник может отследить человека, узнав его внешний **IP-адрес**. На деле не всё так просто – информация о клиентах находится в безопасности у провайдера. Доступ к личным данным такого рода могут получить только органы государственной безопасности.



Единственное, что можно узнать по **IP-адресу**, так это местоположение оборудования провайдера, а такая информация указывает лишь на примерную геолокацию пользователя с точностью до страны и города.

## 6.2. Атака сетевого устройства.

Злоумышленник может обнаружить **IP-адрес** устройства и просканировать его на наличие потенциальных дыр в безопасности. В качестве последних могут выступать брандмауэры со слабой защитой. Также существуют программы, которые прослушивают внешние порты (например, **SSH**, **VNC**, **HTTP**, **RDP**) устройства пользователя на предмет уязвимостей.

Атаки сетевых устройств проводятся как через **Интернет**, так и по локальной сети. Иногда спасает использование **DHCP**, то есть **IP-адрес** меняется при переподключении, поэтому злоумышленнику приходится заново искать **IP-адрес** и начинать атаку.

## 6.3. Фиксация деятельности со стороны провайдера.

**Интернет-провайдер** выступает в роли посредника и может анализировать сетевой трафик. Данные, передающиеся через незашифрованные протоколы (например, **HTTP**, **FTP**), разбираются без проблем. При использовании защищённых вариантов (**HTTPS**, **SFTP**, **SSH**) передаётся информация только об адресе или домене конечного сервера.

Провайдеры не проверяют всех подряд. Подобный анализ трафика выполняется при поступлении запроса со стороны органов безопасности (**МВД**, **ФСБ** и других).

# 7. Способы защиты IP-адреса.

От перечисленных угроз может обезопасить использование **сети TOR**, прокси или **VPN**. Представленные типы защиты выполняют скрытие **IP-адреса**, что анонимизирует деятельность пользователя в сети.

**Сеть TOR** работает по принципу «луковичной маршрутизации», когда пользовательский трафик перенаправляется через несколько серверов-посредников и выходит в **Интернет**. Такой **публичный IP-адрес** пользователя постоянно меняется, что анонимизирует деятельность и не позволяет отследить трафик. Начать использование **сети TOR** можно, скачав официальный браузер **Tor Browser**, который, помимо маршрутизации, блокирует отслеживающие трекеры интернет-ресурсов.

Прокси и **VPN** работают схоже. Трафик перенаправляется через сервер (или несколько серверов) и выходит в **Интернет** с подменой **IP-адреса**.

Технология **VPN**, в отличие от прокси, шифрует данные по пути от пользователя до сервера-посредника, поэтому считается **лучшим вариантом** в плане безопасности.

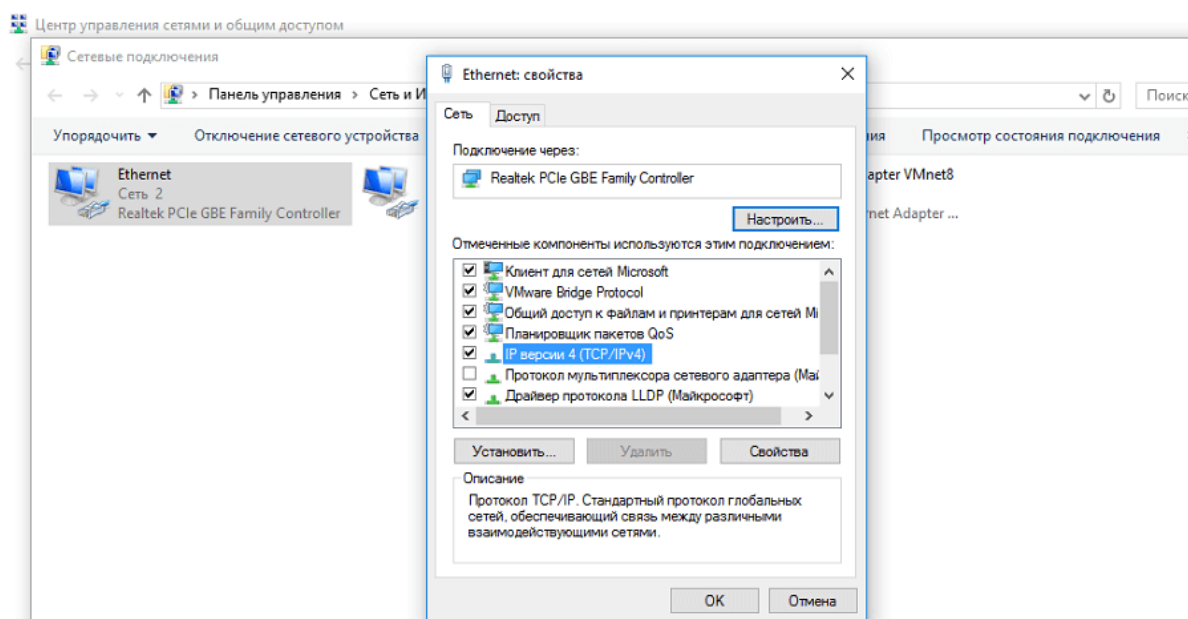
## 8. Как изменить IP-адрес.

### 8.1. Локальная сеть.

Изменение **IP-адреса** выполняется через настройки операционной системы. Далее будут приведены два способа изменения сетевого идентификатора на примере операционных систем **Windows** и **GNU/Linux**.

#### 8.1.1. Windows.

Для начала необходимо открыть **Панель управления** и перейти по пути: **Центр управления сетями и общим доступом** → **Изменение параметров адаптера**.



Далее нужно перейти в свойства необходимого сетевого интерфейса и в появившемся окне открыть свойства компонента **Протокол Интернета версии 4 (TCP/IPv4)**. В разделе **Общие** остаётся назначить **статический IP-адрес**, заполнив все необходимые поля.

#### 8.1.2. GNU/Linux.

В первую очередь нужно посмотреть список подключенных сетевых интерфейсов. Для этого можно воспользоваться консольной командой: `ifconfig`.

```
root@www:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 
          inet addr:          Bcast:          Mask:
          inet6 addr:          Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:941623108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69561577 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:129632183203 (120.7 GiB)  TX bytes:141348431994 (131.6 GiB)
```

Необходимо выбрать сетевой интерфейс и запомнить его наименование.

Теперь стоит ввести следующую команду, чтобы назначить другой **IP-адрес**:

```
# ifconfig eth0 192.168.0.1 netmask 255.255.255.0
```

В приведенном примере:

- eth0 – наименование сетевого интерфейса;
- 192.168.0.1 – назначаемый IP-адрес;
- 255.255.255.0 – маска подсети.

## 8.2. Глобальная сеть.

Многие провайдеры используют динамическое назначение **IP-адреса**, поэтому достаточно перезагрузить маршрутизатор (роутер) для смены сетевого идентификатора.

Если назначен белый **IP-адрес**, то варианты решения проблемы уже другие:

- VPN;
- Прокси;
- Обращение к провайдеру.

Первые два способа были описаны выше – эти варианты являются наиболее простыми. Обращение к провайдеру является крайним вариантом – потребуется совершить звонок по номеру телефона горячей линии или сделать запрос на получение **IP-адреса** в ближайшем филиале.

## 9. Заключение.

В основе **Интернета** и любой **TCP/IP** сети лежит **IP-адресация**. Каждый системный администратор должен знать её основы для построения сетей как в домашней, так и в корпоративной среде.

Не стоит забывать и о безопасности, ведь плохо сконфигурированная сеть имеет уязвимости, позволяющие злоумышленнику нарушить работу

подключения или получить доступ к личной информации.

## **10. Оригиналы источников информации.**

1. [eternalhost.net](http://eternalhost.net) «IP-адрес – что это такое, как его посмотреть и изменить».