Частный IP-адрес

**Частный IP-адрес**[[1]](https://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BD%D1%8B%D0%B9_IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81#cite_note-1)[[2]](https://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BD%D1%8B%D0%B9_IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81#cite_note-2) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *private IP address*), также называемый *внутренним*, *внутрисетевым* или *локальным* — [IP-адрес](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81), принадлежащий к специальному диапазону, не используемому в сети Интернет. Такие адреса предназначены для применения в [локальных сетях](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), распределение таких адресов никем не контролируется. В связи с [дефицитом свободных IP-адресов](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%87%D0%B5%D1%80%D0%BF%D0%B0%D0%BD%D0%B8%D0%B5_IPv4-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%BE%D0%B2), провайдеры всё чаще раздают своим абонентам именно внутрисетевые адреса, а не внешние, при этом они все выходят в интернет через один внешний IP (так называемый «белый IP»).

Иногда частные адреса называют неанонсированными, внешние (так называемые «белые IP») — анонсированными.

Частные диапазоны IP-адресов

Следующие диапазоны определены [IANA](https://ru.wikipedia.org/wiki/IANA) как адреса, выделенные локальным сетям:

[**IPv4**](https://ru.wikipedia.org/wiki/IPv4)

10.0.0.0 — 10.255.255.255 ([маска подсети](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B4%D1%81%D0%B5%D1%82%D0%B8) для бесклассовой ([CIDR](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D1%81%D0%BA%D0%BB%D0%B0%D1%81%D1%81%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0%D1%86%D0%B8%D1%8F)) адресации: 255.0.0.0 или /8)

* 100.64.0.0 — 100.127.255.255 (маска подсети 255.192.0.0 или /10) - Данная подсеть рекомендована согласно RFC 6598 для использования в качестве адресов для CGN (Carrier-Grade NAT).
* 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)

Также для [петлевых интерфейсов](https://ru.wikipedia.org/wiki/Localhost) (не используется для обмена между узлами сети) зарезервирован диапазон 127.0.0.0 — 127.255.255.255 (маска подсети: 255.0.0.0 или /8).

[**IPv6**](https://ru.wikipedia.org/wiki/IPv6)

* fc00::/7 — 7-битный префикс адреса.[[4]](https://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BD%D1%8B%D0%B9_IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81#cite_note-4)

Понятия частных и внешних, статических и динамических адресов

Существует тенденция путать понятия частного IP-адреса и динамического. Ошибочно полагать, что все адреса, выделяемые провайдером динамически — частные, а фиксированные адреса (закреплённые статически) — внешние. Под динамическим *выделением* адреса [узлу сети](https://ru.wikipedia.org/wiki/%D0%A3%D0%B7%D0%B5%D0%BB_%D1%81%D0%B5%D1%82%D0%B8) понимается присвоение нового адреса для каждой сессии соединения ([аренда адреса](https://ru.wikipedia.org/wiki/DHCP#%D0%A0%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%BE%D0%B2), отсутствие постоянно закрепленного за узлом адреса), таким образом присваиваться могут как частные (приватные), так и внешние (публичные) адреса.

Как машины с частными адресами выходят в Интернет

Пакеты, идущие с внутренних IP-адресов или на них, магистральные [маршрутизаторы](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) не пропускают. То есть, внутрисетевые машины, если не принимать никаких мер, изолированы от Интернета. Тем не менее, есть ряд технологий, которые позволяют выходить таким машинам в Интернет.

**Сервер-посредник**

Многие из старых интернет-служб ([электронная почта](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0), [IRC](https://ru.wikipedia.org/wiki/IRC), [Usenet](https://ru.wikipedia.org/wiki/Usenet" \o "Usenet)) специально спроектированы для машин, которые не имеют прямого выхода в Интернет. Для этого в самих протоколах предусмотрена эстафетная передача информации. Рассмотрим её на примере электронной почты.

Корпоративный почтовый сервер имеет два IP-адреса: внутренний и внешний. Для отправки почты пользователь по протоколу [SMTP](https://ru.wikipedia.org/wiki/SMTP) связывается с сервером. Сервер от своего имени выходит в интернет и переправляет почту дальше по цепочке. На этот же сервер по протоколу SMTP поступает входящая корреспонденция. Чтобы проверить ящик, пользователи соединяются с сервером по протоколу [POP3](https://ru.wikipedia.org/wiki/POP3).

Для [Всемирной паутины](https://ru.wikipedia.org/wiki/%D0%92%D1%81%D0%B5%D0%BC%D0%B8%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B0%D1%83%D1%82%D0%B8%D0%BD%D0%B0) была придумана технология «сервер-посредник» (или по-английски «[прокси-сервер](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80)»). Машина с частным адресом обращается к прокси-серверу и посылает на него команды HTTP. Прокси-сервер связывается с веб-сервером от своего имени.

Такая конструкция удовлетворила важнейшие нужды внутрисетевых пользователей. Однако минусом является сложная архитектура сервера-посредника: ведь он должен поддерживать множество разных протоколов. А по протоколам, которые посредник не поддерживает или которые не рассчитаны на эстафетную передачу (например, [сетевые игры](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F_%D0%B8%D0%B3%D1%80%D0%B0)), выход в интернет невозможен. Одни программы ([ICQ](https://ru.wikipedia.org/wiki/ICQ), [Skype](https://ru.wikipedia.org/wiki/Skype" \o "Skype), P2P-часть протокола [BitTorrent](https://ru.wikipedia.org/wiki/BitTorrent_(%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB)" \o "BitTorrent (протокол))) проходят сквозь прокси-серверы, «заворачивая» свой протокол в HTTP-пакеты, другие ([Subversion](https://ru.wikipedia.org/wiki/Subversion" \o "Subversion), связь с трекером в протоколе BitTorrent) — изначально реализуют свой протокол поверх HTTP. Но это всё полумеры. Следующая технология, [NAT](https://ru.wikipedia.org/wiki/NAT), позволила внутрисетевым машинам выходить в интернет по любому прикладному протоколу.

Прокси-серверы работают на [прикладном уровне](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%BF%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F) и потому могут накладывать [цензуру сайтов](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%86%D0%B5%D0%BD%D0%B7%D1%83%D1%80%D0%B0), [кэшировать](https://ru.wikipedia.org/wiki/%D0%9A%D1%8D%D1%88) страницы для экономии трафика — поэтому прокси-серверы применяются в корпоративных сетях и поныне (даже если другие протоколы работают через NAT). Кроме того, серверы-посредники применяются для особых задач, на которые NAT не способен (например, для передачи файлов в [мессенджерах](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BC%D0%B3%D0%BD%D0%BE%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%BC%D0%B5%D0%BD%D0%B0_%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D1%8F%D0%BC%D0%B8" \o "Система мгновенного обмена сообщениями), когда обе машины за NAT’ом).

**Трансляция сетевых адресов (NAT)**

Технология была задокументирована в 1994 году. [Маршрутизатор](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80), реализующий [NAT](https://ru.wikipedia.org/wiki/NAT) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Network Address Translation*), пропуская идущий из локальной сети пакет, заменяет адрес отправителя своим. Когда маршрутизатор получает ответ от сервера, он по таблице открытых соединений восстанавливает адресата и ретранслирует ему ответ.

Через NAT внутрисетевой компьютер может налаживать связь с любым сервером Интернета по любому прикладному протоколу. Но у NAT есть и недостатки. С машиной с частным IP-адресом связаться можно только изнутри локальной сети. С одной стороны, это делает локальную сеть недоступной для многих атак извне. С другой стороны, в некоторых службах Интернета ([одноранговых сетях](https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D1%80%D0%B0%D0%BD%D0%B3%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C" \o "Одноранговая сеть), [сетевых играх](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F_%D0%B8%D0%B3%D1%80%D0%B0), передаче файлов в [мессенджерах](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%81%D1%81%D0%B5%D0%BD%D0%B4%D0%B6%D0%B5%D1%80" \o "Мессенджер)) это создаёт проблемы: если у одного из компьютеров IP-адрес частный, а у другого внешний, инициатором соединения будет клиент с частным IP; если частные у обоих — прямой обмен между ними затруднён. Впрочем, NAT-маршрутизатор может установить [*перенаправление портов*](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BB%D1%8F%D1%86%D0%B8%D1%8F_%D0%BF%D0%BE%D1%80%D1%82-%D0%B0%D0%B4%D1%80%D0%B5%D1%81): когда по определённому порту связываются с маршрутизатором, он передаёт пакеты одной из машин. Обычно порты перенаправляют вручную, настройкой маршрутизатора, но существуют и механизмы автоматического перенаправления портов: [UPnP](https://ru.wikipedia.org/wiki/UPnP" \o "UPnP) и [STUN](https://ru.wikipedia.org/wiki/STUN).

Некоторые протоколы (например, [FTP](https://ru.wikipedia.org/wiki/FTP) в активном режиме) требуют возможности установления соединения от сервера к клиенту. В этих случаях маршрутизатору приходится вмешиваться в протокол на прикладном уровне (технология «[шлюз прикладного уровня](https://ru.wikipedia.org/wiki/%D0%A8%D0%BB%D1%8E%D0%B7_%D0%BF%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F)»).

**Сетевой туннель**

Туннель — технология, когда пакеты [сетевого уровня](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) «заворачиваются» в пакеты более [высоких уровней](https://ru.wikipedia.org/wiki/ISO-OSI) (например, [транспортного](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C)). Это позволяет наладить виртуальную локальную сеть поверх сети совсем другого устройства. Существует много технологий туннелирования ([PPPoE](https://ru.wikipedia.org/wiki/PPPoE" \o "PPPoE), [VPN](https://ru.wikipedia.org/wiki/VPN), [Hamachi](https://ru.wikipedia.org/wiki/Hamachi" \o "Hamachi) и другие), со своими областями применения. В частности, туннели могут:

* Выходить в интернет только тогда, когда пользователь явно этого желает. Такие «непостоянные» соединения были актуальны в [домосетях](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C" \o "Домовая сеть) начала 2000-x годов, когда локальный трафик был дешёвый или бесплатный, внешний — дорог. Чтобы «внутренние» ресурсы не расходовали дорогой трафик, на клиентских машинах приходилось корректировать [таблицу маршрутизации](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8).
* Обеспечивать «прямую» связь внутрисетевых машин друг с другом (например, для сетевых игр), когда прямой путь невозможен. Разумеется, такая «прямая» связь происходит через сервер-посредник.
* Наладить «локальную» сеть для ПО, которое работает на [широковещательных пакетах](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82) — например, для тех же игр.
* Выходить через интернет в корпоративную локальную сеть.