

# Удаленный доступ по белому статическому IP

## Публичные и частные IP-адреса

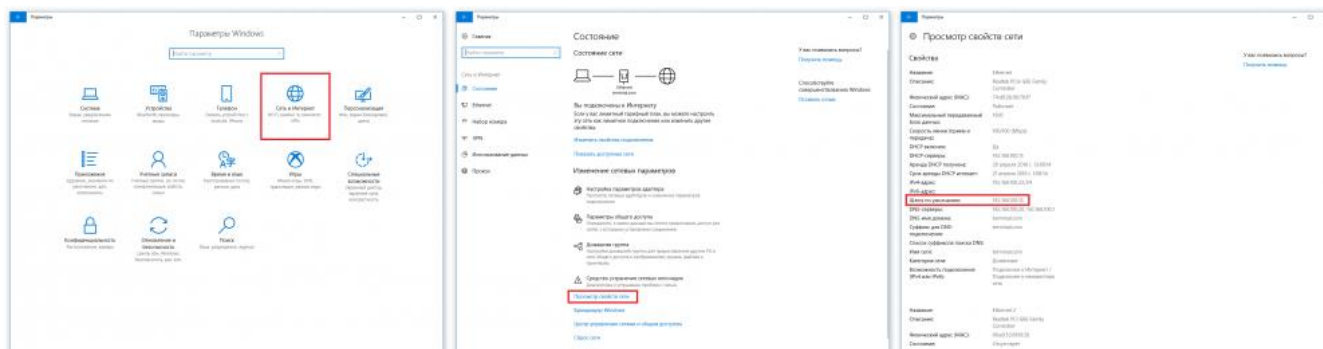
Для постоянного мониторинга объекта через интернет организация удаленного доступа по белому статическому IP-адресу является наилучшим решением в плане надежности и скорости подключения, несмотря на наличие [Облачный\_сервис | других способов] организовать доступ до оборудования **VeSta**.

Существуют два типа IP-адресов - **публичные** («белые») и **частные** («серые»). Публичные IP-адреса используются в сети интернет, а частные - внутри локальных сетей. При предоставлении доступа к интернету поставщик услуг (интернет-провайдер) может выдать публичный или частный IP-адрес. Так как в подавляющем большинстве случаев интернет от провайдера подключается через маршрутизатор, этот IP-адрес будет назначен его **WAN-интерфейсу**. Если IP-адрес частный, то из внешней сети (через интернет) напрямую попасть на маршрутизатор будет нельзя.

Узнать тип внешнего IP-адреса можно двумя способами. Первый - обратиться к интернет-провайдеру. Второй - выяснить самостоятельно через **веб-интерфейс** маршрутизатора:

**1.** Нужно узнать локальный (**LAN**) адрес маршрутизатора. Обычно указан на корпусе маршрутизатора и всегда указан в инструкции.

**1\***. (Опционально) Если локальный адрес был изменен, узнать его можно в сведениях о сетевом подключении компьютера, соединенного с маршрутизатором (для компьютера адрес маршрутизатора является **адресом шлюза**).



Адрес шлюза в Windows 10

- В **Windows 10** для этого следует зайти в «**Параметры Windows**», «**Сеть и Интернет**», в разделе «**Состояние**» выбрать строку «**Просмотр свойств сети**»; среди отображаемых свойств нужно найти строку «**Шлюз по умолчанию**».
- В **Windows 7** и **Windows 8** следует зайти в «**Панель управления**», «**Сеть и Интернет**», «**Центр управления сетями и общим доступом**», «**Изменение параметров адаптера**»; нажать двойным щелчком по используемому подключению, в появившемся окне нажать на «**Сведения**»; среди отображаемых свойств нужно найти строку «**Шлюз по умолчанию**».

**2.** Следует перейти по адресу шлюза в браузере (ссылка вида «<http://192.168.1.1/>», где 192.168.1.1 - адрес шлюза), при этом должен быть загружен веб-интерфейс маршрутизатора. Логин и пароль по умолчанию обычно указан на корпусе маршрутизатора и всегда указан в инструкции. После входа в веб-интерфейс следует открыть раздел «**Информация**» или «**Статус**», где указаны данные о текущем подключении. IP-адрес интерфейса **WAN** - это внешний IP-адрес маршрутизатора. Если данный IP-адрес имеет вид **10.xxx.xxx.xxx**, **192.168.xxx.xxx** или **172.16.xxx.xxx - 172.31.xxx.xxx**, то у маршрутизатора **частный** («серый») внешний IP-адрес. В иных случаях IP-адрес **публичный** («белый»).

OpenWrt Статус Система Сервисы Сеть Выйти АВТОСОХРАНЕНИЕ ВЫКЛЮЧЕНО

### Статус

#### Система

|                  |   |
|------------------|---|
| Имя хоста        | OpenWrt   |
| Модель           | D-Link DIR-320 B1   |
| Версия прошивки  | OpenWrt Attitude Adjustment 12.09-rc1 / LuCI Trunk (svn-r183) |
| Версия ядра      | 3.3.8   |
| Местное время    | Mon Apr 23 03:18:56 2018                                      |
| Время работы     | 44d 9h 58m 6s   |
| Средняя нагрузка | 1.07, 0.34, 0.17  |

#### Память

|                |                           |
|----------------|---------------------------|
| Всего доступно | 13392 kB / 29940 kB (44%) |
| Свободно       | 5492 kB / 29940 kB (18%)  |
| Кэшировано     | 5784 kB / 29940 kB (19%)  |
| Буферизировано | 2116 kB / 29940 kB (7%)   |

#### Сеть

|                 |   |
|-----------------|---|
| Статус IPv4 WAN | Тип: dhcp<br>eth0: Адрес: 192.168.100.28<br>Маска сети: 255.255.255.0<br>Шлюз: 192.168.100.15<br>DNS 1: 192.168.100.1<br>DNS 2: 192.168.100.20<br>Подключен: 44d 9h 58m 52s |
|-----------------|---|

IP-адрес интерфейса WAN маршрутизатора с прошивкой OpenWRT. В данном случае IP-адрес частный («серый»).

Если IP-адрес публичный, можно приступить к настройке **переадресации портов**. В зависимости от модели маршрутизатора осуществить переадресацию чаще всего можно при помощи функций «Межсетевой экран», «Firewall», «Перенаправление портов» «Виртуальные серверы» или «Port Forwarding».

### Создание правил перенаправления портов

В нашем случае маршрутизатор является **шлюзом**, разделяющим локальную сеть и интернет. У него имеются два интерфейса с со своими IP-адресами: **LAN** (локальный, внутренний) и **WAN** (внешний). Суть перенаправления («**проброса**») портов в рассматриваемой задаче заключается в том, что какому-либо TCP или UDP порту внешнего WAN-интерфейса маршрутизатора ставится в соответствие TCP или UDP порт и IP-адрес какого-либо устройства в локальной сети, например, видеорегистратора. Таким образом, все запросы из внешней сети, адресованные на данный порт маршрутизатора, будут автоматически переадресованы соответствующему порту видеорегистратора в локальной сети.

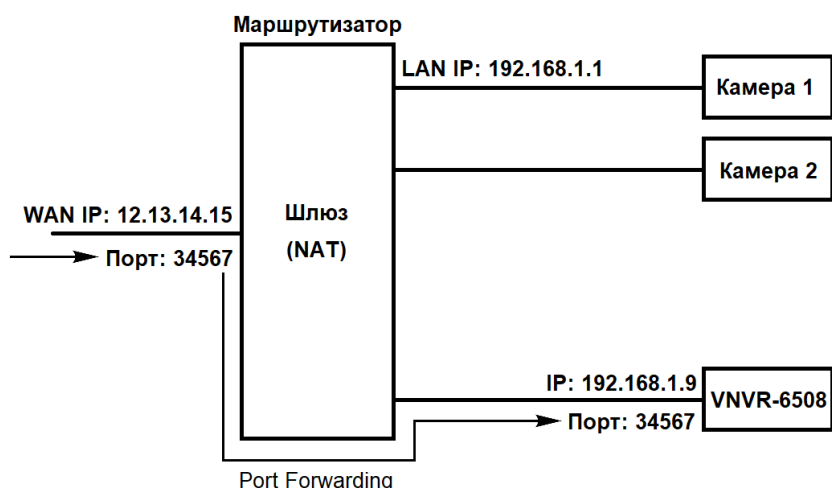
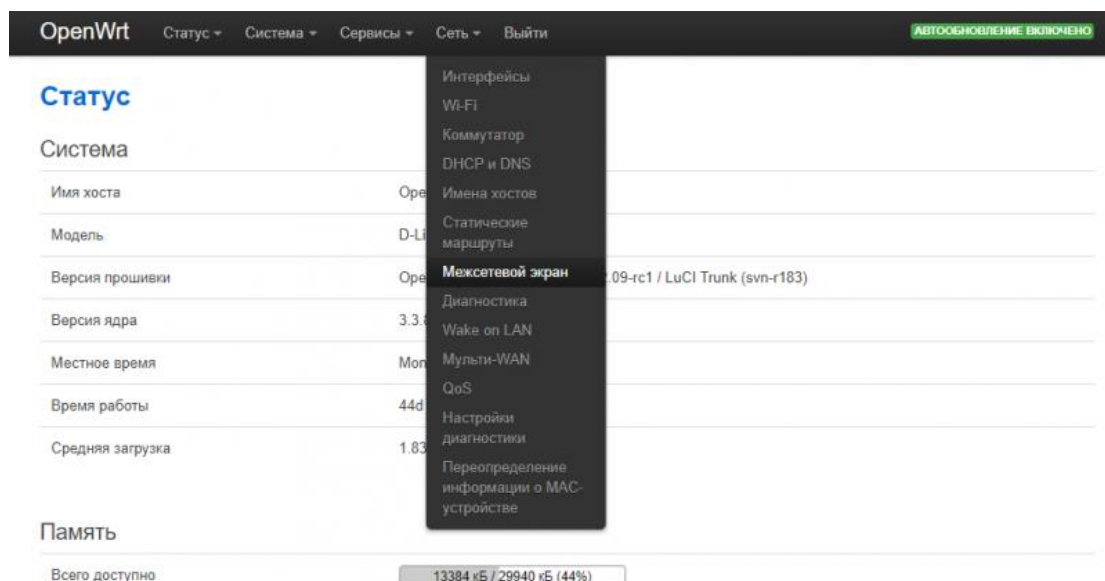


Схема простейшей локальной сети с шлюзом и настроенной переадресацией портов. Запрос, поступивший на порт 34567 внешнего IP-адреса маршрутизатора перенаправляется на порт 34567 устройства в локальной сети с адресом 192.168.1.9

Рассмотрим настройку перенаправления портов на примере маршрутизатора **D-Link** с прошивкой **OpenWRT**.

1. В веб-интерфейсе маршрутизатора следует перейти в раздел «Сеть» - «Межсетевой экран».

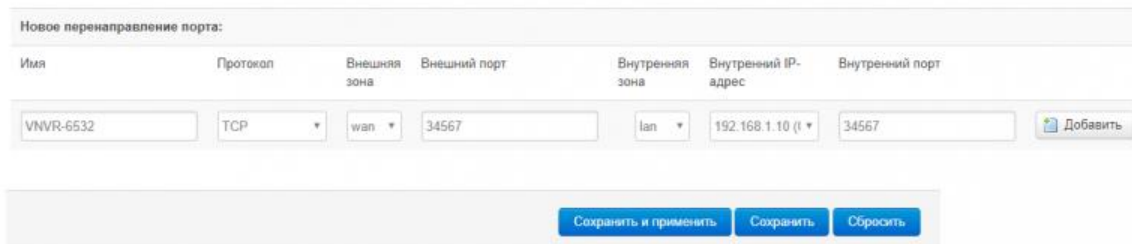


Межсетевой экран в OpenWRT

2. Выбрать подраздел «**Перенаправление портов**». В строке «**Новое перенаправление порта**» следует ввести:

- **Имя:** произвольное.
- **Протокол:** TCP.
- **Внешняя зона:** WAN (выбрать текущее подключение к интернету).
- **Внешний порт:** 34567 (можно выбрать любой другой до 65535; именно этот номер порта будет использоваться для удаленного подключения в дальнейшем).
- **Внутренняя зона:** LAN.

- **Внутренний IP-адрес:** IP-адрес устройства, до которого настраивается удаленный доступ (например, 192.168.1.10).
- **Внутренний порт:** 34567 (порт устройства, до которого настраивается удаленный доступ).



Создание нового правила перенаправления портов в OpenWRT

3. Выбрать «Добавить», а затем «Сохранить и применить параметры». В результате правило перенаправления будет добавлено в список и начнет работать.

### Примечания

- Данное руководство предназначено в первую очередь для пользователей, слабо знакомых с сетевыми технологиями. Многие понятия и определения были заведомо упрощены.
- Данное руководство подходит для настройки перенаправления портов в простейших сетях. При установке оборудования в функционирующей локальной сети предприятия настоятельно рекомендуется для настройки удаленного доступа обратиться к системному администратору, обслуживающему сеть.
- Настройка перенаправления портов осуществляется по-разному для различных моделей маршрутизаторов. Если в веб-интерфейсе вашего маршрутизатора отсутствуют настройки, подобные приведенным в данном руководстве, попробуйте поискать в интернете «**Проброс портов на [модель маршрутизатора]**».
- На некоторых моделях маршрутизаторов при настройке правил перенаправления нельзя отдельно указать внешний и внутренний порт. В этом случае просто укажите порт 34567. Если требуется настроить удаленный доступ сразу до нескольких устройств локальной сети, придется поменять порты устройств через их сетевые настройки.
- Узнавать тип IP-адреса через сервисы наподобие 2ip.ru бессмысленно, так как они всегда отображают публичный (белый) IP-адрес, даже если провайдер предоставляет вам частный (серый) IP-адрес. Отображаемый публичный IP-адрес в этом случае принадлежит оборудованию провайдера.
- В сетевых настройках устройства, до которого настраивается удаленный доступ, в качестве **адреса шлюза** обязательно должен быть указан **IP-адрес маршрутизатора**, на котором настроено перенаправление портов.
- При настройке удаленного доступа до устройства через публичный IP-адрес настоятельно рекомендуется задать на нем надежный пароль.