В этой статье

Железная связь

Как научиться тонкой настройке роутера? Мы поможем разобраться с особенностями конфигурации самого простого и недорогого устройства — D-Link DI-604.

ФИЗИЧЕСКОЕ ПОДКЛЮЧЕНИЕ

Разбираемся с кабелями

Первый этап настройки — это правильное подключение самого устройства.

CHIP Вывод

■ D-Link DI-604 — маршрутизатор «для ленивых». Главное, что от вас потребуется, — это правильно сконфигурировать его всего один раз: после грамотной настройки про это сетевое устройство можно забыть. Вспомнить о существовании роутера придется только в том случае, если ваша сеть разрастется до 15–20 ПК. Вот тогда уже производительности этого роутера окажется недостаточно, и вам нужно будет поменять его на более серьезное устройство.

К гнезду, которое обозначено на роутере как «WAN», необходимо подключить сетевой кабель со стороны провайдера, а вот тот патч-корд надо одним концом подсоединить к порту DI-604, обозначенному цифрой «1», а другим — к сетевой плате на компьютере.

После подключения сетевых кабелей наступает ответственный момент — подсоединение к сети. Если все проделано правильно, то на лицевой панели маршрутизатора DI-604 будут гореть, как минимум, три зеленых огонька. Если не горит ни одного, внимательно поверьте цепь питания. Если не горит лампочка «WAN», обратитесь к своему интернет-провайдеру — пусть он протестирует физическую линию вашего подключения. Если не горит индикатор «1», внимательно проверьте ваш патч-корд.

НАСТРОЙКА СЕТЕВОЙ ПЛАТЫ

Если не срабатывает автоматика

Теперь нам надо подключиться к панели управления маршрутизатором. Для этого необходимо в свойствах протокола TCP/IP сетевой платы вашего компьютера выставить опцию «Получить IP-адрес автоматически». Последовательность действий следующая: «Пуск | Настройка | Сетевые подключения». Здесь вы находите значок «Подключение по локальной сети», кликаете по нему правой кнопкой мыши и выбираете в меню «Свойства». В открывшемся окне из списка «Компоненты, используемые этим подключением» выбираете «Протокол Интернета (TCP/IP)» и

жмете кнопку «Свойства». В окне настроек выбираете закладку «Общие» и устанавливаете здесь следующие значения: «Получить IP-адрес автоматически», «Получить адрес DNS-сервера автоматически». Для проверки правильности этой настройки надо выполнить команду: «Пуск | Настройка | Сетевые подключения», кликнуть по значку «Подключение по локальной сети» правой кнопкой мыши и в появившемся меню выбрать пункт «Состояние». Далее в открывшемся окне надо выбрать закладку «Поддержка» и посмотреть на полученный IP-адрес: он должен представлять собой набор цифр «192.168.0.X», где вместо X обычно находится 2.

Если по каким-то причинам ваш компьютер не смог получить IP-адрес автоматически, то необходимо назначить его в явном виде. Для этого выполните последовательность команд: «Пуск | Настройка | Сетевые подключения | Подключение по локальной сети | Свойства | Компоненты, используемые этим подключением | Протокол Интернета (TCP/IP) | Свойства». В открывшемся окне нужно установить следующие значения:

- ✔ IP-адрес: 192.168.0.2;
- ✔ маска подсети: 255.255.255.0;
- ✔ шлюз по умолчанию: 192.168.0.1;
- ✔ адреса DNS-серверов: 192.168.0.1.

ПЕРВИЧНАЯ НАСТРОЙКА РОУТЕРА

Что делать с мастером?

Следующий шаг — подключение к панели управления. Для этого откройте интернет-браузер (MS Internet Explorer, Mozilla и пр.) и введите в адресной строке «http://192.168.0.1». В появившемся окне ввода пароля наберите «Login: admin», а поле пароля оставьте пустым. В результате вы должны увидеть в окне браузера картинку, которая обычно радует любого пользователя, но слабо утешает сетевого специалиста. Прежде чем начинать работать с ней, лучше всего отключить от устройства кабель, предназначенный для гнезда WAN. Во многих случаях это будет перестраховкой, но зачем искать себе дополнительные проблемы?

D-LINK DI-604 При правильном физическом подключении роутера на панели должны гореть три зеленых индикатора

После отключения внешнего канала у вас есть два варианта: либо вы честно пытаетесь разобраться в настройках роутера, следуя нашим советам, либо просто жмете на кнопку «Run Wizard», запуская мастер первоначальной настройки. В отрывшемся окне кликните по кнопке «Next». Далее вам надо будет два раза ввести новый пароль (в полях «New Password» и «Reconfirm»). Следующим шагом будет указание «TimeZone».

ВНИМАНИЕ После смены пароля при переходе к окну «Choose Time Zone» вам необходимо будет снова ввести пароль, только на этот раз надо будет набрать новый пароль — именно тот, который вы два раза ввели на предыдущем шаге. Конечно, «TimeZone» можно и пропустить, но лучше все-таки выбрать нужную временную зону: для Москвы это будет «GMT +03:00».

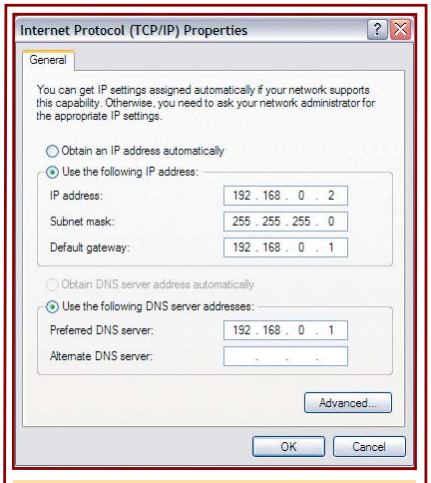
После того, как вы посмотрите на надпись «Auto Detecting WAN», мастер настройки надо закрыть кнопкой «Exit». Конечно, можно и далее проводить настройки с помощью мастера, однако, как показывает практика, гораздо правильнее настраивать любой маршрутизатор без его помощи, как это делаем мы.

ПОДКЛЮЧЕНИЕ К ИНТЕРНЕТУ

Выходим во внешний мир

Способ настройки внешнего канала целиком и полностью зависит от тех данных, которые при подключении к Интернету обязан выдать ваш провайдер. Внешнее подключение настраивается на вкладке «Home» в разделе «WAN». Если вы отключали кабель от порта WAN на время смены пароля, то самое время подключить его обратно.

В самом простом случае провайдером будет ваш умный сосед, который организовал где-то в своей квартире DHCP-сервер и подключил вас именно к нему (вариант небольшой локальной сети). В этом случае вы просто выбираете «Dynamic IP Address», для надежности выбираете в самой нижней строке «Auto- ➜



НАСТРОЙКА ПРОТОКОЛА TCP/IP Для подключения ПК к маршрутизатору D-Link нужно ввести следующие данные

ДОСТУП К РОУТЕРУ В целях безопасности обязательно смените пароль, стоящий на D-Link по умолчанию

КНОПКА «RESET»

Вернуться к началу

В случае серьезных сбоев можно сделать сброс установок к заводским. Данная процедура может производиться двумя способами. Первый — нажать кнопку «Reset to Default» в разделе «System» на вкладке «Tools». Все, казалось бы, просто, но если вы потеряли пароль окончательно, то доступа на эту вкладку у вас не будет. Тогда можно попытаться сбросить установки с помощью кнопки «Reset», которая находится рядом с разъемом питания. Процедура сброса такова:

✔ включаем устройство и ждем порядка 20 с для завершения загрузки;

✔ нажимаем кнопку «Reset» и держим ее примерно 10-12 с;

✔ отпускаем кнопку — при этом по мигании индикаторов видно, что устройство выполняет перезагрузку.

Иногда, когда к устройству ничего не подключено, отследить мигание индикаторов довольно трудно. Поэтому лучше поступить следующим образом: назначить дополнительный IP-адрес своему сетевому адаптеру из той же подсети, что и адрес по умолчанию у шлюза (то есть, если адрес шлюза по умолчанию 192.168.0.1, то надо добавить, например, 192.168.0.10).

Затем нажимаем «Пуск | Выполнить» и набираем команду ping -t 192.168.0.1. После этого откроется окно вывода результатов команды, в котором с интервалом примерно в 1 с будут появляться строчки «Request timed out».

Теперь выполняем аппаратный сброс, и если все было сделано верно, ваш маршрутизатор начнет отвечать на команду ping и сообщения, например, поменяются на такие:

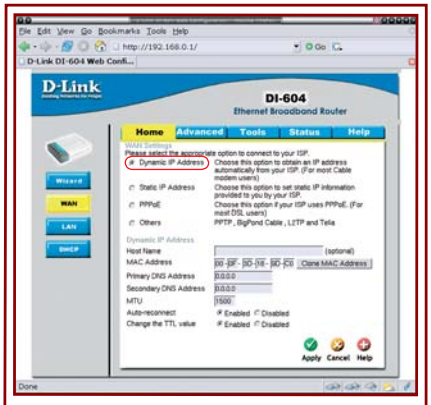
✔ **Reply from 192.168.0.1**: bytes=32 time<1ms TTL=64

✔ **Reply from 192.168.0.1**: bytes=32 time<1ms TTL=64

✔ **Reply from 192.168.0.1**: bytes=32 time<1ms TTL=64

✔ **Reply from 192.168.0.1**: bytes=32 time<1ms TTL=64

После завершения перезагрузки получаем устройство с настройками по умолчанию (заводскими установками).



DYNAMIC IP ADDRESS При автоматическом получении IP-адреса ничего настраивать не придется

reconnect» в пункт «Enable», нажимаете кнопку «Apply» и после перезагрузки роутера получаете готовое подключение к Интернету.

СОВЕТ ОТ ТЕХПОДДЕРЖКИ D-LINK В этом случае у провайдера обычно IP-адрес привязывается к MAC-адресу сетевой платы ПК, поэтому будет не лишним нажать кнопку «Clone MAC».

Назначение статического IP-адреса — это более сложный случай в настройке. Выбор варианта «Static IP Address» в том же разделе «WAN» подразумевает ввод всех атрибутов IP-адресации: адрес («IP Address»), маска подсети («Subnet Mask»), шлюз по умолчанию («ISP Gateway Address»), адреса DNS-серверов («Primary DNS Address», «Secondary DNS Address») и «MTU». Последнее поле, если нет прямого указания провайдера, можно оставить со значением, принятым по умолчанию — «1500». После того как роутер перезагрузится, все должно заработать.

И, наконец, самый сложный вариант настройки — VPN-подключение. К сожалению, на сегодняшний день тут нет универсального решения. Каждый провайдер вправе реализовывать наиболее удобный, с его точки зрения, способ. Типичным можно считать вариант реализации VPN от Corbina Telecom, который мы опишем далее.

Для подключения к «Корбине» в разделе «WAN» надо выбрать неочевидную для многих опцию «Others», которая, кстати говоря, дает расширенные варианты настройки.

Далее выполняем алгоритм.

✔ **«Dynamic IP»** — «Корбина» отдает пользовательские адреса автоматически по DHCP, поэтому поля «My IP Address», «My Subnet Mask» и «My Gateway» становятся в этом случае для заполнения недоступны.

✔ **«Server IP/Name»** — для Москвы этот адрес один: «vpn.corbina.net».

✔ **«PPTP Account»** — тут надо ввести ваш логин.

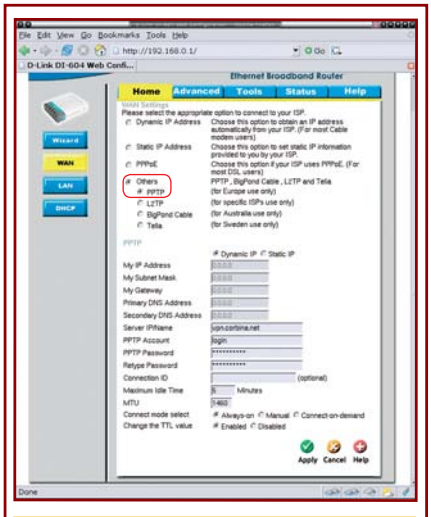
✔ **«PPTP Password»** — вводим свой пароль.

✔ **«Retype Password»** — повторяем ввод пароля.

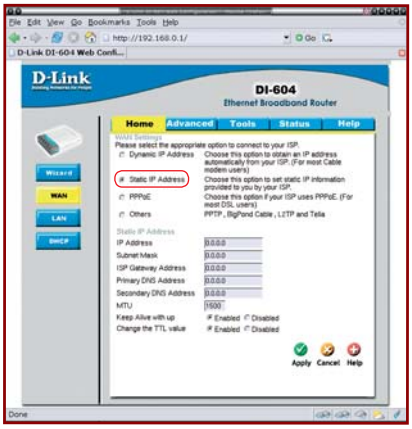
✔ **«Maximum Idle Time» и «MTU»** — следует оставить эти значения по умолчанию.

✔ **«Connect mode select»** — выбор этой функции зависит от вас. Если вы хотите, чтобы ваше соединение было постоянно включено, поставьте значение «Always-on»; «Manual» означает, что вам придется включать это соединение каждый раз вручную; а выбор варианта «Connect-on-demand» заставит роутер самостоятельно создавать соединение, как только возникнет необходимость выхода в Сеть.

Необходимо сказать несколько слов о внутренних ресурсах локальной сети. Можно, конечно, для их использования отключать Интернет, но это очень неудобно. В роутере скрыта возможность настройки одновременного использования Интернета и ресурсов



VPN Самым сложным вариантом настройки является VPN-подключение



STATIC IP ADDRESS Ручная настройка подразумевает ввод всех атрибутов IP-адресации

общей локальной сети. И хотя в данном случае речь будет идти о внутренних ресурсах «Корбины», в общем случае все это можно проделать с любым другим оператором.

Наберите в адресной строке браузера «http://192.168.0.1/rtab.htm», и вы попадете в недокументированную настройку маршрутизации роутера.

В поля с заголовком «Destination» вводим адреса сетей «Корбины»:

- ✔ Локальная сеть: 10.0.0.0-255.0.0.0
- ✔ Сервер статистики: 195.14.50.26-255.255.255.255
- ✔ Почтовый сервер: 195.14.50.16-255.255.255.255
- ✔ Локальные ресурсы: 85.21.79.0-255.255.255.0, 85.21.90.0-255.255.255.0
- ✔ Corbina.TV: 85.21.52.254-255.255.255.255, 85.21.88.130-255.255.255.255, 83.102.146.96-255.255.255.224

В поле с заголовком «Gateway» вводим IP-адрес шлюза, получаемый по DHCP при подключении компьютера напрямую — выглядеть он должен как «10.X.X.X». Его можно получить, позвонив в техподдержку интернет-провайдера. Далее везде ставим галочки и нажимаем кнопку «Apply».

НАСТРОЙКИ LAN

Смотрим внутрь

Хотя настройки по умолчанию, касающиеся внутренней сети («LAN Setting»), для большинства приложений достаточно удобные и не требуют ничего кроме ознакомления, в некоторых случаях вам захочется их изменить. В большей степени это касается настроек DHCP-сервера. Вы можете, например, решить, чтобы каждому пользователю внутренней сети назначался только определенный IP-адрес. Это бывает необходимо, когда требуется считать трафик отдельно для каждого пользователя небольшой офисной сети. Модель DI-604 сама по себе считать трафик не умеет, но это может сделать какая-нибудь специальная программа на вашем компьютере.

Для реализации этой задачи необходимо выбрать вкладку «Home» и нажать кнопку «DHCP». В этом разделе настраивается DCHP-сервер. В верхней части окна расположены основные настройки сервера: его включение («DCHP Server Enable» или «Disable»), диапазон выдаваемых адресов (начало — «Starting IP Address», конец — «Ending IP Address») и время жизни IP-адреса (по умолчанию одна неделя).

В нижней части окна — конфигурация «замораживания» IP-адресов. Здесь вы можете назначить на MAC-адрес сетевой платы клиента определенный IP-адрес. Настройка здесь очевидна.

- ✔ **«Name»** — обозначение клиента.
- ✔ **«IP Address»** — назначаемый адрес.
- ✔ **«MAC Address»** — параметры сетевой карты можно узнать, если выполнить на клиентском компьютере следующую последовательность действий: «Пуск | Настройка | Сетевые подключения | Подключение по локальной сети | Состояние | Поддержка | Подробности». В открывшемся окне запомните, а лучше запишите шесть шестнадцатеричных цифр и введите их последовательно в шесть окошек в панели управления роутером.

После этой процедуры нажмите кнопку «Apply» и ждите перезагрузки. ➜

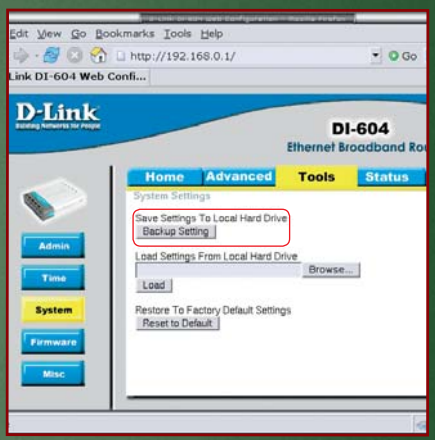
BACKUP SETTINGS

Обновляем, сохраняем, восстанавливаем

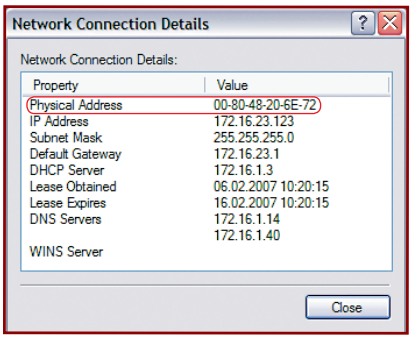
Роутер D-Link DI-604, как и всякое серьезное оборудование, обладает возможностью сохранения и восстановления конфигурационной информации, а также обновления внутренней прошивки. Все эти функции расположены на вкладке «Tools».

Чтобы сохранить текущую конфигурацию, нажимаем кнопку «System», потом «Backup Settings» и указываем место на жестком диске, куда желательно сохранить конфигурационные данные. Восстановление идентично, за исключением того, что сначала надо выбрать файл, а потом уже запустить процесс восстановления.

Тут же, на вкладке «Tools», расположена и кнопка «Firmware», с помощью которой можно обновить прошивку роутера. Если вы все-таки решитесь на такой ответственный шаг, то имейте в виду, что если в процессе прошивки вдруг отключится электричество, помочь вам смогут только в специализированном техническом центре. Новую прошивку можно скачать по адресу **ftp://ftp.dlink.ru/pub/Router/DI-604/Firmware**, ознакомившись предварительно со списком всего, что там есть, и выбрав прошивку именно для вашей версии маршрутизатора. Для роутеров DI-604 версии могут начинаться с букв B, D, F или E. Точную версию можно посмотреть на самом устройстве снизу.



BACKUP SETTINGS позволит сохранить и восстановить удачную конфигурацию вашего роутера



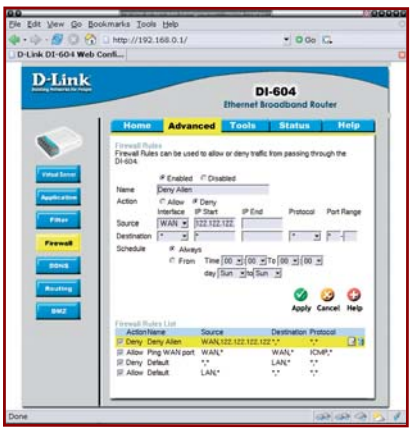
MAC ADDRESS Физический адрес своей сетевой платы можно узнать в свойствах локального подключения

ЗАЩИТА ОТ ВТОРЖЕНИЯ

Продвинутые настройки

Если вдруг вы заподозрили, что роутер подвергся нападению некоего внешнего злоумышленника, то самое время заняться настройкой встроенного брандмауэра. Лучше всего, если вы сумеете определить IP-адрес злодея. Хорошим подспорьем для этого может стать лог роутера, доступный на вкладке «Misc» по кнопке «Logs».

Предположим, что вам по какой-то причине, например, не понравился адрес «122.122.122.122», и вы желаете закрыть доступ с этого IP на ваш маршрутизатор раз и навсегда. Чтобы решить эту проблему, зайдите на панель управления роутером, выберите вкладку «Advanced» и нажмите кнопку «Firewall». Далее следует произвести логичные и простые действия.



FIREWALL Вы можете закрыть доступ на маршрутизатор с конкретного IP-адреса

✔ **«Enable»** — включаем правило.
✔ **«Name»** — пишем его внутреннее имя, например, «DenyAlien».
✔ **«Action»** — «Allow», если разрешаем прохождение пакетов; «Deny», если запрещаем. В данном случае мы выбираем «Deny».
✔ **«Source»** — источник пакетов. Тут можно задать либо интерфейс, откуда пакеты приходят (если из Интернета, то «WAN»), либо конкретный IP-адрес, либо диапазон адресов. Мы выбираем «WAN» и указываем IP-адрес 122.122.122.122.
✔ **«Destination»** — приемник. Дальше действуем, как и с опцией «Source» (указываем «WAN» — для запрета доступа снаружи).
✔ **«Protocol»** — варианты выбора здесь стандартные: «TCP», «UDP», «ICMP» или все возможные. Последний вариант обозначен «звездочкой» (*) — его мы и выбираем.
✔ **«Port Range»** — «1-65535».
✔ **«Schedule»** — расписание. Лучше выбрать пункт «Always» — всегда. Здесь можно указать и конкретное время работы данного правила.

ВИРТУАЛЬНЫЕ СЕРВЕРЫ

Настраиваем работу веб-сервера

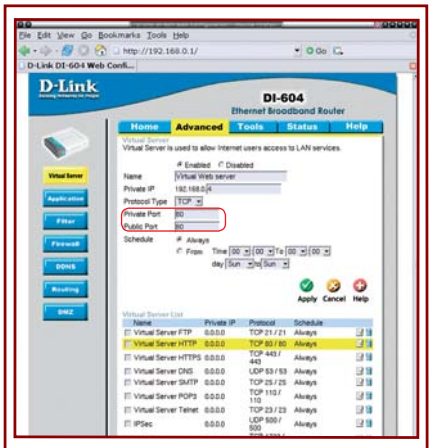
Предположим, что вы решили создать собственный веб-сервер и выложить некоторые материалы для всеобщего использования. Сделать это довольно просто — прежде всего, надо поднять на одной из внутренних машин (пусть это будет компьютер с адресом 192.168.0.4) веб-сервер (например, Apache, хотя можно обойтись и встроенным в Windows сервером IIS 5.1) и настроить его по вашему усмотрению. Далее надо «пробросить» порт 80 протокола TCP сквозь ваш роутер напрямую на внутренний адрес. Делается это так (вкладка «Advanced», закладка «Virtual Servers»):
✔ **«Enable»** — включаем «проброс» порта.
✔ **«Name»** — пишем внутреннее имя сервиса, например «VirtualWebServer».
✔ **«Private IP»** — внутренний адрес сервера.
✔ **«ProtocolType»** — для веб-сервера будет «TCP», для других возможны варианты «UDP» и «Both» (то есть оба протокола).
✔ **«Private Port»** — порт, на котором работает веб-сервер на внутренней машине (обычно 80).
✔ **«Public Port»** — порт, который будет виден как порт вашего веб-сервера снаружи: 80.
✔ **«Schedule»** — расписание остается на ваше усмотрение, хотя лучше, если веб-сервер будет всегда доступен пользователям.

Теперь нажмите кнопку «Apply», перезагрузите систему, и ваш сайт станет доступным для интернет-пользователей.

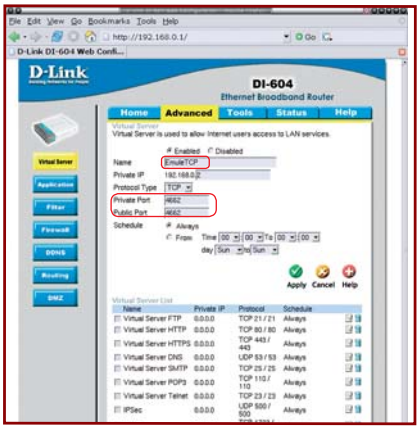
Чтобы настроить DI-604 для работы, например, с E-Mule, надо открыть для прямого доступа из WAN порты 4662 TCP и 4672 UDP. Предполагаем, что эта программа живет на внутреннем IP-адресе 192.168.0.2. Конфигурирование здесь аналогично «пробрасыванию» внутрь сети 80-го порта для веб-сервера.

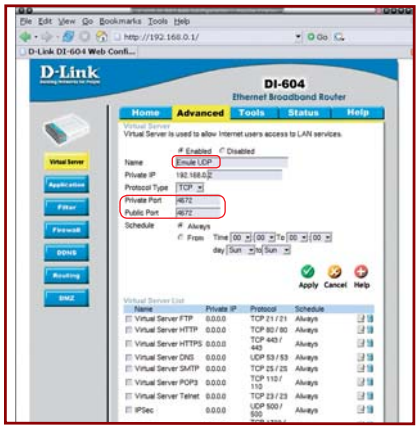
Для порта 4662 TCP — вкладка «Advanced», закладка «Virtual Servers».
✔ **«Enable»** — включаем.
✔ **«Name»** — «EmuleTCP».
✔ **«Private IP»** — внутренний адрес сервера: «192.168.0.2».
✔ **«Protocol Type»** — «TCP».
✔ **«Private Port»** — «4662».
✔ **«Public Port»** — «4662».
✔ **«Schedule»** — «Allways».

Для порта 4672 UDP — вкладка «Advanced», закладка «Virtual Servers».

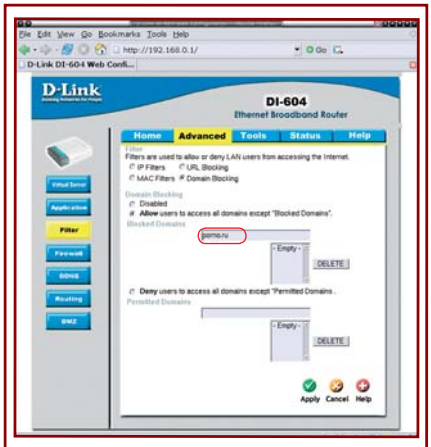


VIRTUAL SERVERS «Пробрасываем» порт 80 протокола TCP сквозь роутер напрямую на внутренний адрес





ДЛЯ РАБОТЫ С E-MULE открываем для доступа из WAN порты 4662 TCP и 4672 UDP



DOMAIN BLOCKING — самый удобный вариант блокировки из четырех возможных

✔ **«Enable»** — включаем.
✔ **«Name»** — «EmuleUDP»
✔ **«Private IP»** — внутренний адрес сервера: «192.168.0.2».
✔ **«Protocol Type»** — «UDP».
✔ **«Private Port»** — «4672».
✔ **«Public Port»** — «4672».
✔ **«Schedule»** — «Allways».

ЗАКРЫВАЕМ ДОСТУП НА ДОМЕНЫ

Фильтры и запреты

Довольно часто возникает ситуация, когда пользователям LAN необходимо закрыть доступ на некоторые IP-адреса или сетевые домены. Например, нужно заблокировать все адреса домена **porno.ru** для локальных пользователей. Чтобы это реализовать, необходимо использовать механизм фильтров. Для этого откройте вкладку «Advanced» и нажмите «Filters». Вариантов блокировки четыре.

✔ **«IP Filters»** — при выборе этого варианта необходимо заполнить поля «IP Address», «Port Range» и «Protocol» указав, соответственно, диапазон IP-адресов, номера портов и наименования тех протоколов, которые вы хотите заблокировать.
✔ **«URL Blocking»** — в этом варианте блокировки достаточно ввести полный адрес того ресурса, доступ на который необходимо запретить.
✔ **«MAC Filters»** — здесь вы можете запретить доступ компьютерам с определенными MAC-адресами сетевых плат. Просто введите имя пользователя и MAC-адрес его сетевой карты.
✔ **«Domain Blocking»** — удобный вариант блокировки. Вы можете либо разрешить доступ ко всем доменам, кроме запрещенных (опция «Allow users to access all domains except «Blocked Domains»), либо наоборот — запретить доступ ко всем кроме разрешенных.

По общему шаблону

В сетевых устройствах других производителей будет несколько иное расположение разделов настройки в панели управления, однако все операции можно провести по аналогии с теми действиями, которые мы описали на примере D-Link. Положим, что в вашем случае настройки DHCP-сервера будут расположены не в закладке «DHCP», а в разделе «Basic», однако и там вы найдете те же самые опции: «DCHP Server Enable», «Disable», «Starting IP Address», с которыми можно работать по нашим алгоритмам.

■ ■ ■ **Сергей Кондращев**

DMZ

Свободная буферная зона

Роутер DI-604 обладает еще одной важной функцией, использование которой может помочь вам не только защитить свою внутреннюю сеть от возможного вторжения, но и организовать мониторинг попыток такого вторжения абсолютно безопасно для остальной сети. Речь идет о создании демилитаризованных зон (DMZ). Под этим термином понимается некое пространство внутренней сети, которое будет изолировано от остальной части LAN и одновременно видно из внешней сети.
Для организации DMZ зайдите на вкладку «Advanced» и нажмите кнопку «DMZ», а дальше просто введите адрес компьютера, который вы хотите ввести в DMZ. Включите правило, выбрав опцию «Enable», и демилитаризованная зона готова. Теперь все запросы, приходящие на внешний адрес, будут автоматически направляться на машину, находящуюся в демилитаризованной зоне.

DMZ Свободная буферная зона поможет организовать мониторинг попыток вторжения