DD-WRT Общие Заметки

Активация параметра Boot Wait для защиты от повреждения устройства

По умолчанию для доступа к маршрутизатору используется учетная запись root / admin, а его IP-адрес устанавливается в 192.168.1.1, поэтому для запуска Web-интерфейса DD-WRT необходимо в Web-браузере на ближайшем компьютере ввести URL-адрес http://192.168.1.1.

Прежде чем приступать к любым действиям, необходимо зайти на страницу **Administration** (администрирование) > **Management** (управление) и убедиться, что параметр **Boot Wait** включен, как показано на рисунке 1.

Рисунок 1. Параметр Boot Wait должен быть всегда в состоянии Enable

Этот параметр по умолчанию должен быть включен, так как он обеспечивает пятисекундную задержку при загрузке устройства. Поэтому если устройство по какой либо причине не загружается, то у вас будет пять секунд чтобы заново загрузить прошивку из флэш-памяти. Это действие обеспечивает дополнительную защиту от выхода из строя маршрутизатора.

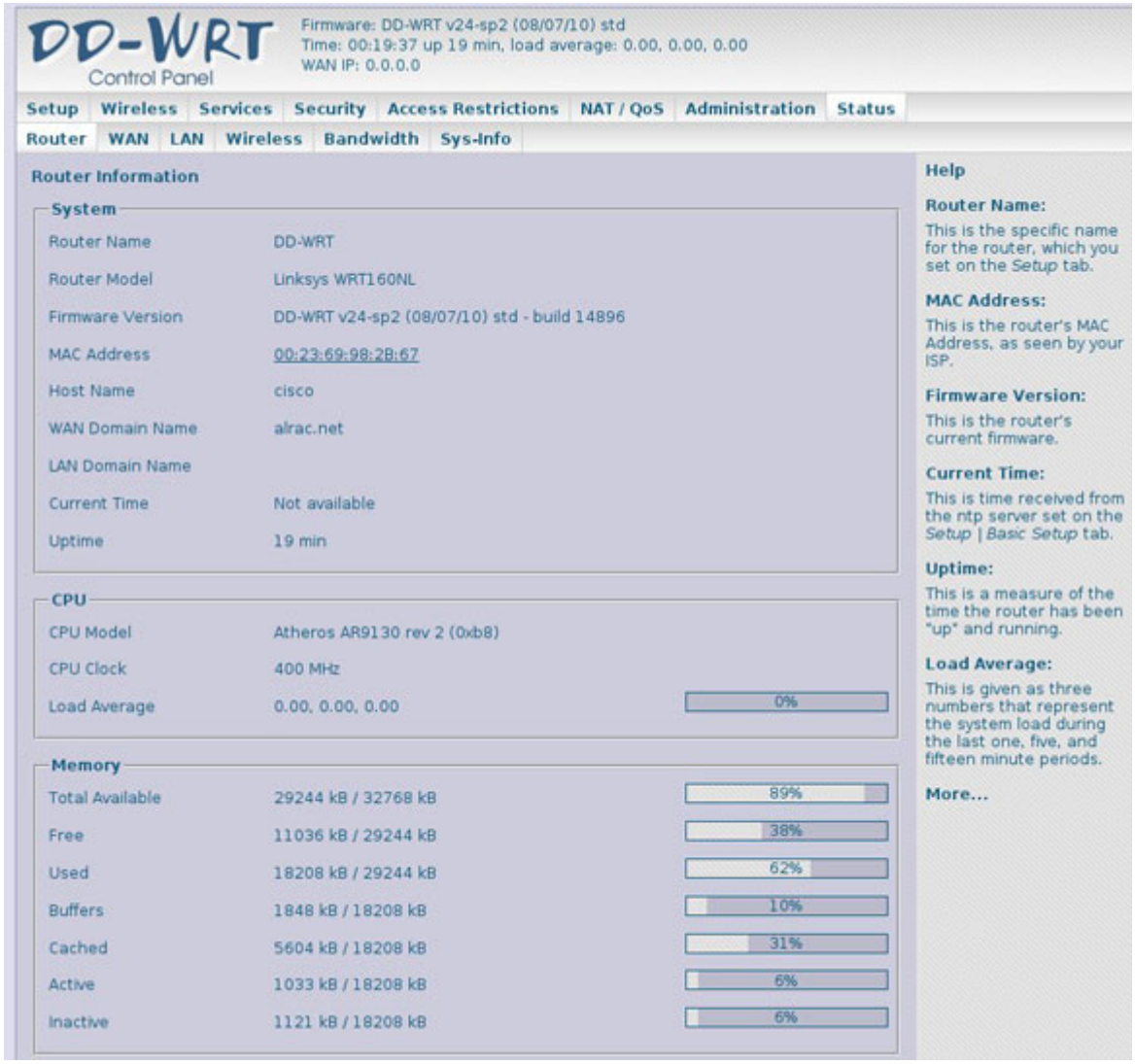
Различия между опциями Save, Apply Settings и Reboot Router

На каждой странице с опциями для изменения конфигурации в Web-интерфейсе внизу имеются кнопки **Save** (сохранить) и **Apply Settings** (применить настройки), а иногда еще и кнопка **Reboot Router** (перегрузить маршрутизатор). Кнопка **Save** сохраняет ваши изменения, не применяя их, так что они не будут активированы до тех пор, пока маршрутизатор не будет перезагружен. Кнопка **Apply Settings** сохраняет изменения и немедленно применяет их, при необходимости перезапуская службы. Кнопка **Reboot Router** предназначена для изменений, требующих перезагрузки, поэтому необходимо их предварительно сохранить.

Защищенное общение с маршрутизатором

Большинство административных задач можно выполнять через Web-интерфейс DD-WRT, который обладает всеми нужными функциями и аккуратно построен. На рисунке 2 показан пример Web-интерфейса моего маршрутизатора. Здесь можно увидеть увеличенный рисунок 2.

Рисунок 2. Web-интерфейс DD-WRT содержит большое количество информации о конфигурации и состоянии устройства



По умолчанию Web-интерфейс использует протокол HTTP, в котором информация передается открытым текстом, так что доступ к административному интерфейсу следует защитить, переключившись на протокол HTTPS на странице **Administration** (администрирование) > **Management** (управление) > **Web Access** (Web-доступ). Нажмите на кнопку **Apply Settings** для немедленного сохранения и активации изменений, а потом перезапустите Web-браузер и откройте адрес https://192.168.1.1 (или другой IP-адрес, который используется вашим устройством).

В первый раз вам будет показано предупреждение о сертификате Web-сайта, который был подтвержден NewMedia-NET GmbH. Подтвердите подлинность этого сертификата, чтобы Web-браузер сохранил его локально. В будущем вы сможете сами выступить в роли сертифицирующего органа и сгенерировать свой собственный сертификат, правда, этот вопрос выходит за рамки данной статьи.

Также администрирование DD-WRT можно выполнять из командной строки, что даёт доступ к конфигурационным возможностям, не поддерживаемым Web-интерфейсом. Это также еще одна возможность для управления маршрутизатором, если Web-интерфейс перестанет работать. По умолчанию используется протокол Telnet, а не SSH. Обратиться к маршрутизатору по протоколу Telnet можно следующим образом:

```
$ telnet 192.168.1.1
DD-WRT login: root
Password:
```

В качестве имени пользователя всегда должен использовать root, в независимости от того, какое имя пользователя вы установили раньше, а пароль должен быть именно тот, который был установлен вами. Для выхода из telnet-сеанса необходимо ввести `exit`. Использование telnet допустимо на этапе знакомства с DD-WRT, но поскольку этот протокол не обладает никакой защитой, необходимо отключить его и перейти на SSL, когда вы начнете использовать маршрутизатор в рабочем режиме. Для этого необходимо перейти на страницу **Services** (службы) > **Services** в Web-интерфейсе, как показано на рисунке 3.

Рисунок 3. Отключение Telnet и активация SSH

После нажатия на кнопку **Apply Settings** вы сможете подключиться к DD-WRT уже через SSH. Как и раньше используется имя пользователя root и фактический пароль.

```
$ ssh root@192.168.1.1

DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH
Release: 08/07/10 (SVN revision: 14896)
root@192.168.1.1's password:
=====================================================


 _____  ___    __          ______ _____          ____  _  _
 | _ \| _ \   \ \       / /  _ \_   _| __   _|___ \| || |
 || | || ||____\ \ /\ / /| |_) || |   \ \ / / __) | || |_
 ||_| ||_||_____\ V  V / |  _ < | |    \ V / / __/|__   _|
 |___/|___/      \_/\_/  |_| \_\|_|     \_/ |_____|  |_|

                     DD-WRT v24-sp2
                  http://www.dd-wrt.com

=====================================================


BusyBox v1.13.4 (2010-08-07 05:06:30 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

Пример команд:

```
nvram set httpd_enable=1
nvram set http_enable=1
nvram set http_lanport=80
nvram set httpsd_enable=1
nvram set https_enable=1
nvram set http_wanport=8080

nvram commit

reboot
```

Хотите добиться ещё большей безопасности? Тогда настройте вход с использованием открытого ключа и без использования пароля – это защитит от попыток взлома перебором паролей и никто не сможет войти в систему, не имея копии закрытого ключа. Сначала нужно создать зашифрованную пару ключей, на Linux это можно сделать с помощью команды `ssh-keygen`.

```
$ ssh-keygen -t rsa -C router1 -f ~/.ssh/linksys
```

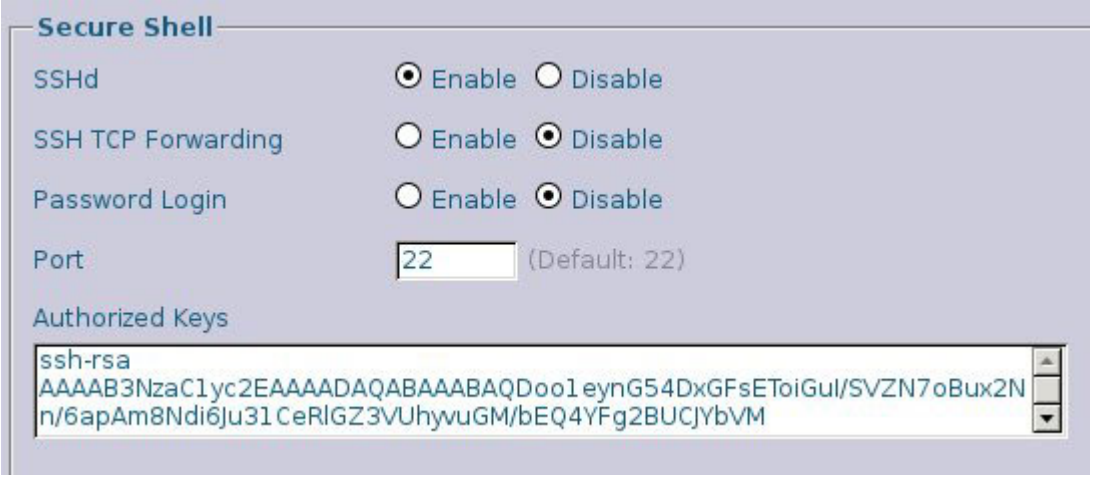
В этом примере создаётся пара RSA-ключей с названием **linksys**. Открытый ключ называется **linksys.pub**, а закрытый **linksys** и оба хранятся в каталоге **~/.ssh**, стандартном месте для хранения SSH-ключей, хотя вы можете хранить свои ключи и в другом месте. Далее в файл **/etc/ssh/ssh_config** необходимо добавить строку для идентификации данных ключей.

```
IdentityFile ~/.ssh/linksys
```

Параметр `-C` добавляет комментарий внутрь файла с открытым ключом, который на самом деле является обычным текстовым файлом. Впоследствии по этому комментарию я при необходимости смогу идентифицировать данный ключ.

Теперь необходимо скопировать созданный открытый ключ на DD-WRT устройство, поместив содержимое файла с ключом в текстовое поле, находящееся в разделе SSH на странице **Services** > **Services** и отключить вход с помощью пароля, как показано на рисунке 4.

Рисунок 4. Копирование открытого SSH-ключа для аутентификации на DD-WRT-устройстве



Остается нажать кнопку **Save**, а затем кнопку **Reboot Router**. Если у вас уже была открытая SSH-сессия, то она автоматически будет закрыта, а при следующем входе в систему пароль уже проверяться не будет. Если необходимо добавить несколько ключей, то они должны разделяться символом переноса строки.

Эти же действия можно выполнить и из командной строки, используя команду `nvram`. Убедитесь, что ваш открытый ключ в виде единой строки полностью находится в одинарных кавычках (в теле ключа могут встречаться пробелы, но не символы переноса строки).

```
root@linksys:~# nvram set sshd_authorized_keys='ssh-rsa AAAAB3NzaC...89Suj
router1'
root@linksys:~# nvram commit
root@linksys:~# reboot
```

При использовании `nvram` также можно установить несколько ключей, поместив отдельные ключи в кавычки и разделив их пробелами.

```
root@linksys:~# nvram set sshd_authorized_keys='key1' 'key2' 'key3'
root@linksys:~# nvram commit
```

Желательно сначала ввести необходимый текст в текстовом редакторе, чтобы убедиться, что в нём нет ошибок, а затем целиком скопировать его и вставить в командную строку.

Команда nvram

Термин **nvram** имеет несколько значений. Во-первых, это сокращение от non-volatile RAM, специального типа энергонезависимой памяти, сохраняющей данные при отключении питания. Флеш-память, используемая в маршрутизаторе, как раз относится к типу **nvram**. Команда `nvram` используется для управления настройками аппаратного обеспечения, которые хранятся в последнем блоке флеш-памяти. Этот сегмент памяти часто также называется **nvram**. Различные версии команды `nvram` учитывают специфику продуктов IBM, CISCO, Oracle и Apple. Версия команды nvram, используемой DD-WRT может только выводить и изменять значения, присвоенные переменным, а также удалять переменные. Если запустить её без указания опций, то будут выведены возможные опции и пример синтаксиса использования.

```
root@linksys:~# nvram
usage: nvram [get name] [set name=value] [unset name] [show]
```

Команда `nvram` с параметром `show` выводит все доступные настройки вашего маршрутизатора. Вы можете использовать команду `less`, чтобы разделить имеющуюся информацию и выводить её постранично.

```
root@linksys:~# nvram show | less
```

Или найти определенную переменную с помощью утилиты `grep`, как показано ниже.

```
root@linksys:~# nvram show | grep ssh
```

Совет: если вы случайно отключите Web-интерфейс, но сохраните возможность подключения через telnet или SSH, то Web-интерфейс можно включить следующим способом.

```
root@linksys:~# nvram set http_enable=1
root@linksys:~# nvram commit
root@linksys:~# reboot
```

Это изменение будет применено после перезагрузки. Значение параметра `boot_wait` нельзя изменить через GUI, но с помощью `nvram` это возможно. Сначала необходимо узнать текущее значение данного параметра.

```
root@linksys:/etc# nvram show |grep wait
boot_wait=on
wait_time=5
```

Так как я крайне осторожна, то предпочту увеличить это значение до 10 секунд.

```
root@linksys:/etc# nvram set wait_time=10
root@linksys:~# nvram commit
```

Стереть уже установленное значение переменной также очень просто.

```
root@linksys:~# nvram set http_enable=""
root@linksys:~# nvram commit
```

Если вы не хотите, чтобы какое-то изменение можно было отменить, перезагрузив маршрутизатор, то просто не пользуйтесь командой `nvram commit`. Это хороший приём, который позволяет проводить эксперименты, так как достаточно просто перегрузить маршрутизатор, чтобы вернуться к предыдущему состоянию.

Команда `nvram unset [variable]` полностью удаляет указанную переменную. На ресурсе OpenWrt Wiki можно найти хорошее описание команды nvram (см. раздел "Ресурсы").

Последним шансом на исправление испорченной конфигурации может стать сброс всех настроек маршрутизатора в значения по умолчанию, установленные в прошивке. Для этого необходимо нажать кнопку сброса (reset) на маршрутизаторе и удерживать её в течении 30 секунд, а затем перегрузить устройство. После этого будут восстановлены значения по умолчанию DD-WRT, а не оригинальной прошивки устройства, как ошибочно предполагают некоторые пользователи.

Создание второго раздела

Стандартный образ DD-WRT занимает раздел размером в 4 МБ, даже если размер флеш-памяти равен 8 МБ или больше. Поэтому на данном неиспользуемом пространстве можно создать раздел и использовать его для хранения файлов. Этот раздел должен использоваться в основном для считывания информации, например, активности беспроводной точки доступа, страниц с конфигурацией и Web-страниц, дополнительных конфигурационных файлов, а также для хранения ipkg (Itsy Package Management System - система управления пакетами, предназначенная для встроенных устройств). Не стоит использовать эту область для хранения файлов, в которые будет вестись интенсивная запись информации, например, журнальных файлов, так как флеш-память поддерживает только определенное количество циклов записи и поэтому может внезапно отказать. Хотя современная флеш-память достаточно надёжна, но всё же количество возможных циклов записи для неё ограничено. Информацию о текущей файловой системы можно получить с помощью известной команды `df`:

```
root@linksys:/# df -h
Filesystem                Size      Used Available Use% Mounted on
/dev/root                 4.0M      4.0M         0 100% /
```

В моём маршрутизаторе имеется 8МБ флеш-памяти, но, как мы видим, из них используется только 4 МБ, хотя остальные 4 МБ можно также использовать. Для этого в Web-интерфейсе необходимо открыть Web-страницу **Administration** (администрирование) > **Management** (управление) и выбрать опции **JFFS2** > **Enable** (включить) и **Clean JFFS2** (очистить JFFS2) > **Enable**. После этого необходимо щелкнуть кнопки **Apply Settings** и **Reboot Router**. После перезагрудки маршрутизатора вывод команды `df` должен выглядеть, как показано ниже.

```
root@linksys:~# df -h
Filesystem                Size      Used Available Use% Mounted on
/dev/root                 4.0M      4.0M         0 100% /
/dev/mtdblock/3           2.3M    196.0K      2.1M   9% /jffs
```

JFFS2 — это журналируемая файловая система для флеш-памяти (Journalling Flash File System version 2), спроектированная для устройств хранения данных на основе флеш-памяти. Необходимо сделать небольшое отступление и рассказать, что такое флеш-память. Это специальное устройство, называемое MTD (Memory Technology Device). MTD – это не блочное устройство, в отличии от жестких дисков или USB-накопителей, но и не символьное устройство, как клавиатура или мышь. Блочные устройства построены на основе секторов фиксированного размера, например 512 или 1024 байта. В MTD-устройствах используются специальные "стираемые" блоки (eraseblock) размером 128 КБ или больше. Блочные устройства умеют делать две вещи: считывать и записывать сектора. MTD-устройства обладают большими возможностями: они могут считывать, записывать и «стирать» блоки.

Карты памяти Compact Flash и SD, USB-флешки на самом нижнем уровне также являются MTD-устройствами. Но для операционной системы они выглядят как блочные устройства, так как они используют технологию FTL (Flash Translation Layers — поуровневое преобразование флеш-памяти), которая эмулирует поведение блочного устройства поверх аппаратной флеш-памяти. Технология FTL может применяться в компьютере или в самом устройстве, в прошивке его контроллера. Если вы попробуете разобрать USB-накопитель, то, скорее всего, обнаружите в нём несколько NAND-чипов, которые и являются флеш-памятью, и микроконтроллер.

Для успешной работы с DD-WRT желательно знать несколько особенностей функционирования флеш-памяти. Во-первых, стираемые блоки NAND являются «атомарными», т.е. всё содержимое блока должно быть стёрто, прежде чем туда можно будет записать новые данные. Во-вторых, в Linux имеется подсистема MTD и команда `mtd`, позволяющие выполнять основные задачи, например, запись образа на устройство или его очистку. Чтобы получить информацию о синтаксисе и опциях команды `mtd`, её можно запустить на DD-WRT-устройстве без указания параметров. В DD-WRT WiKi также можно найти информацию и инструкции по работе с `mtd`. В-третьих, команда nvram располагается в самом последнем блоке и её размер программно ограничен 32 КБ, в независимости от того каков реальный размер блока.

Советы по работе с командной строкой

Эти советы помогут освоить возможности DD-WRT:

- DD-WRT построена на основе BusyBox, широко известного набора инструментов Linux для встраиваемых устройств. В BusyBox содержатся "урезанные" версии основных утилит Linux. Для экономии пространства в BusyBox отсутствуют страницы справочника `man`, но узнать о командах BusyBox, также называемых апплетами, можно с помощью команды `man busybox` (см. раздел "Ресурсы"). Можно запустить команду `ls -l /bin` (или **/sbin** или **/usr/bin**) для просмотра содержимого каталогов, содержащих исполняемые файлы, чтобы узнать какие команды будут доступны в BusyBox по известным символическим ссылкам.

- В DD-WRT используется оболочка **ash**, поставляемая с BusyBox. Список команд, встроенных в оболочку, можно вывести с помощью команды `builtin`.
- Также как и на больших Linux-системах, вы можете считывать информацию из файловых систем **/proc** и **/sys**, чтобы узнать больше об аппаратном обеспечении, а конфигурационную информацию можно найти в файловой системе **/etc**.