Прошиваем DD-WRT в D-Link DIR-300

По мотивам: http://www.dd-wrt.com/wiki/index.php/Прошивка_DIR-300

Подготовка

Узнаем что будем перешивать

Первое что нужно сделать - это узнать номер ревизии маршрутизатора (наклейка на обратной стороне).

У меня такая железка: D-Link DIR-300 H/W Version: A1, F/W: 1.03

Все дальнейшее описание прошивки предполагается что ревизия маршрутизатора A1. Для ревизии B1 способ прошивки несколько иной, читать тут: http://sergey-s-betke.blogs.novgaro.ru/networking/devices/d-link/dap-1150/proshivaem-d-link-proshivkoj-dd-wrt

Качаем необходимые файлы

Идем на http://www.dd-wrt.com/site/support/router-database ищем наш маршрутизатор, качаем файлы

- ap61.ram
- ap61.rom
- linux.bin

Устанавливаем TFTP-сервер

Процедура прошивки проводилась на компьютере с OS Ubuntu. Требуется установленный TFTP-сервер.

```
$ sudo apt-get install tftp tftpd
```

Если необходимо - вносим изменения в конфигурационный файл /etc/inetd.conf

Складываем нужные нас файлы в папку /srv/tftp

Запускаем сервис

```
$ sudo service openbsd-inetd start
```

Если работаем на Windows, то рекомендую http://tftpd32.jounin.net/

Перепрошивка

Включаем сетевой кабель в порт «INTERNET» (он же WAN), вторым концом в компьютер.

Отключаем питание D-link, зажимаем кнопку Reset, включаем питание. Через 30 сек отпускаем кнопку Reset.

Устанавливаем на компьютере новый IP-адрес:

```
$ sudo ifconfig eth0 192.168.20.80
```

Подключаемся к D-link:

```
$ telnet 192.168.20.81 9000
Trying 192.168.20.81...
Connected to 192.168.20.81.
Escape character is '^]'.
```

Нажимаем Enter, появляется приглашение. Вводим команду

```
RedBoot> load ap61.ram
Using default protocol (TFTP)
Entry point: 0x800410bc, address range: 0x80041000-0x800680d8
```

И вводим

```
RedBoot> go
```

Telnet-сессия или зависнет или оторвется - это нормально.

НЕ выключая и НЕ перегружая маршрутизатор, переключаем кабель в разъем LAN1.

Меняем IP-адрес компьютера:

```
$ sudo ifconfig eth0 192.168.1.2
```

И снова подключаемся к D-link

```
$ telnet 192.168.1.1 9000
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
DD-WRT>
```

Делаем следующее (примечание: выполнение команды fis занимает некоторое время, не нужно паниковать):

```
DD-WRT> fconfig -i
Initialize non-volatile configuration - continue (y/n)? Y
```

```
Run script at boot: false
Use BOOTP for network configuration: true
Default server IP address:
Console baud rate: 9600
GDB connection port: 9000
Force console for special debug messages: false
Network debug at boot time: false
Update RedBoot non-volatile configuration - continue (y/n)? Y
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> fis init
About to initialize [format] FLASH image system - continue (y/n)? Y
*** Initialize FLASH Image System
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> ip_address -h 192.168.1.2
IP: 192.168.1.1/255.255.255.0, Gateway: 0.0.0.0
Default server: 192.168.1.2

DD-WRT> load -r -b %{FREEMEMLO} ap61.rom
Using default protocol (TFTP)
Raw file loaded 0x80080000-0x800a8717, assumed entry at 0x80080000

DD-WRT> fis create -l 0x30000 -e 0xbfc00000 RedBoot
An image named 'RedBoot' exists - continue (y/n)? Y
... Erase from 0xbfc00000-0xbfc30000: ...
... Program from 0x80080000-0x800a8718 at 0xbfc00000: ...
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> reset
```

После этого D-link перезагрузится и сессия прервется. Снова подключаемся телнетом к адресу 192.168.1.1 порт 9000 после того, как маршрутизатор перезапустится и будет ждать команд (на это нужно примерно 30 секунд).

```
$ telnet 192.168.1.1 9000
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

DD-WRT> ip_address -h 192.168.1.2
IP: 192.168.1.1/255.255.255.0, Gateway: 0.0.0.0
Default server: 192.168.1.2

DD-WRT> fis init
About to initialize [format] FLASH image system - continue (y/n)? y
*** Initialize FLASH Image System
... Erase from 0xbffe0000-0xbfff0000: .
```

```
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> load -r -b 0x80041000 linux.bin
Using default protocol (TFTP)
Raw file loaded 0x80041000-0x803ddfff, assumed entry at 0x80041000
DD-WRT> fis create linux
... Erase from 0xbfc30000-0xbffcd000:
.....................................................
... Program from 0x80041000-0x803de000 at 0xbfc30000:
.....................................................
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> fconfig boot_script true
boot_script: Setting to true
Update RedBoot non-volatile configuration - continue (y/n)? Y
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> fconfig boot_script_timeout 3
boot_script_timeout: Setting to 3
Update RedBoot non-volatile configuration - continue (y/n)? Y
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> fconfig bootp false
bootp: Setting to false
Update RedBoot non-volatile configuration - continue (y/n)? Y
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .

DD-WRT> fconfig bootp false
bootp: Setting to false

DD-WRT> fconfig
Run script at boot: true
Boot script:
Enter script, terminate with empty line
>> fis load -l vmlinux.bin.17
>> exec
>>
Enter script, terminate with empty line
>> fis load -l linux
>> exec
>>
Boot script timeout (1000ms resolution): 3
Use BOOTP for network configuration: false
Gateway IP address:
Local IP address:
Local IP address mask:
Default server IP address:
```

```
Console baud rate: 9600
GDB connection port: 9000
Force console for special debug messages: false
Network debug at boot time: false
Update RedBoot non-volatile configuration - continue (y/n)? Y
... Erase from 0xbffe0000-0xbfff0000: .
... Program from 0x80ff0000-0x81000000 at 0xbffe0000: .
DD-WRT> ip_address -h 192.168.1.1
IP: 192.168.1.1/255.255.255.0, Gateway: 0.0.0.0
Default server: 192.168.1.1

DD-WRT> reset
```

Теперь D-link перезагрузится и некоторое время будет недоступен.

Как загорится значок WAN - можно коннектиться браузером на 192.168.1.1. Имя пользователя и пароль по умолчанию - «root» и «admin» соответственно.

Удаленно сбрасываем пароль админа на оригинальной прошивке

Вход в администрирование без ввода пароля:

http://192.168.0.1/bsc_lan.php?NO_NEED_AUTH=1&AUTH_GROUP=0

Сброс пароля на дефолтный удаленным способом:

- http://slrz.ru/2011/09/sbros-parolya-na-routere-dlink-dir-300-dir-320-dir-615/
- http://dl.packetstormsecurity.net/1012-exploits/dlink_php_vulnerability.pdf

dlink, dir-300, dd-wrt, перепрошивка