Восстановление роутер (TP-Link) через Serial

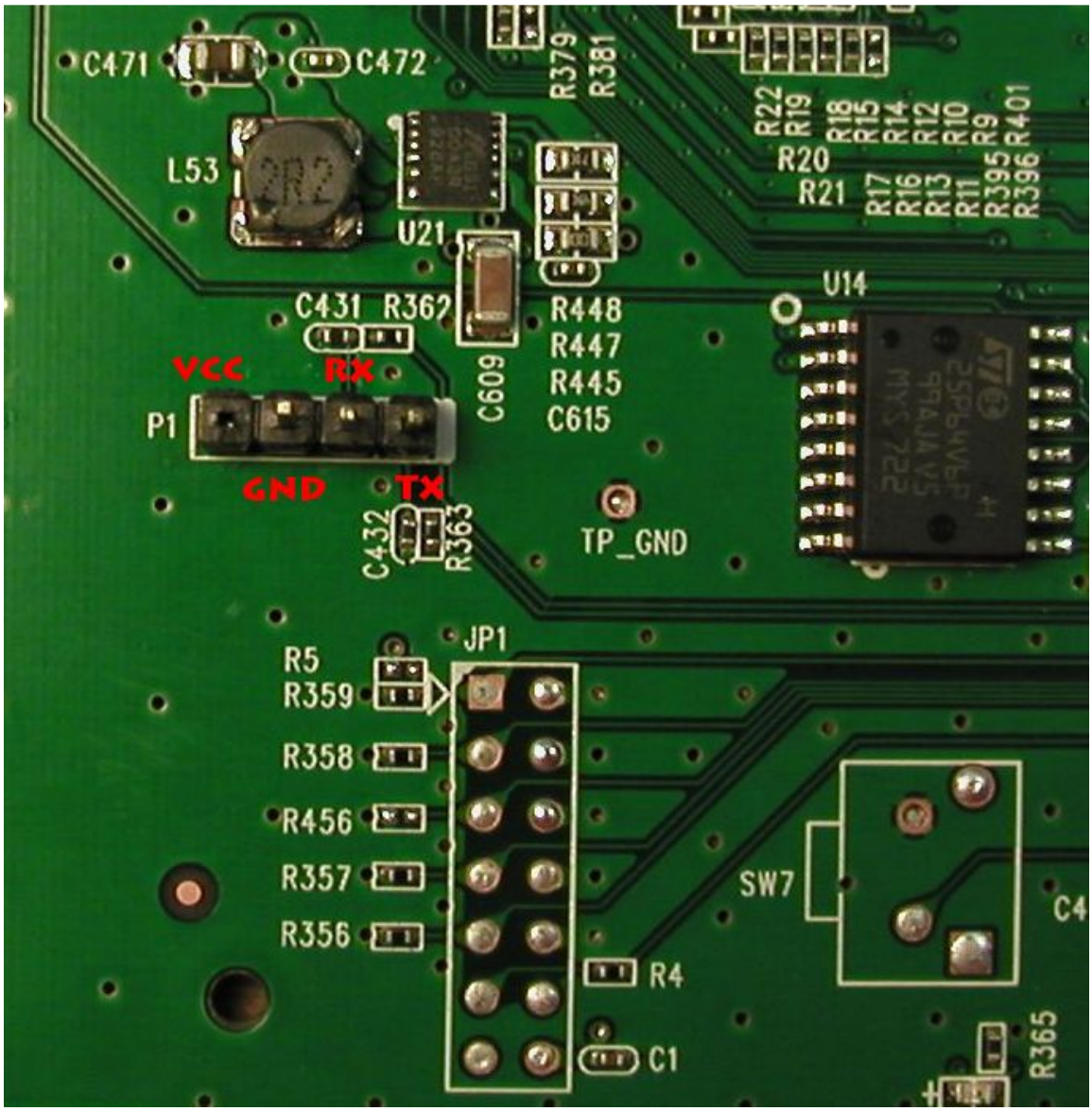
!!!Все ниже описанное вы делаете на свой страх и риск, ни каких гарантий я не даю!!!

Вступление

В этой статье я изложу свой опыт по восстановлению своего роутера TP-Link TL-WR1043ND после полного стирания прошивки или ее повреждения.

И так что мы имеем в самом начале – роутер TP-Link TL-WR1043ND с полностью стертой или поврежденной прошивкой. Симптомы: на роутере горит только индикатор питания, остальные индикатор одновременно загораются и тухнут через 1 сек, при подключению роутера к ПК подключение по локальной сети выдает что сетевой кабель не подключен. Соответственно роутер не доступен не через веб-интерфейс, telnet и ssh.

Теперь роутер можно восстановить 2 способами: использовать программатор и подключиться к роутеру использую разъем на плате **serial** (4 pin) или **JTAG** (14 pin). Программатор в нашем городе я не нашел, поэтому выбрал на второй способ. Для подключения был выбрал 4 контактный разъем **serial**.

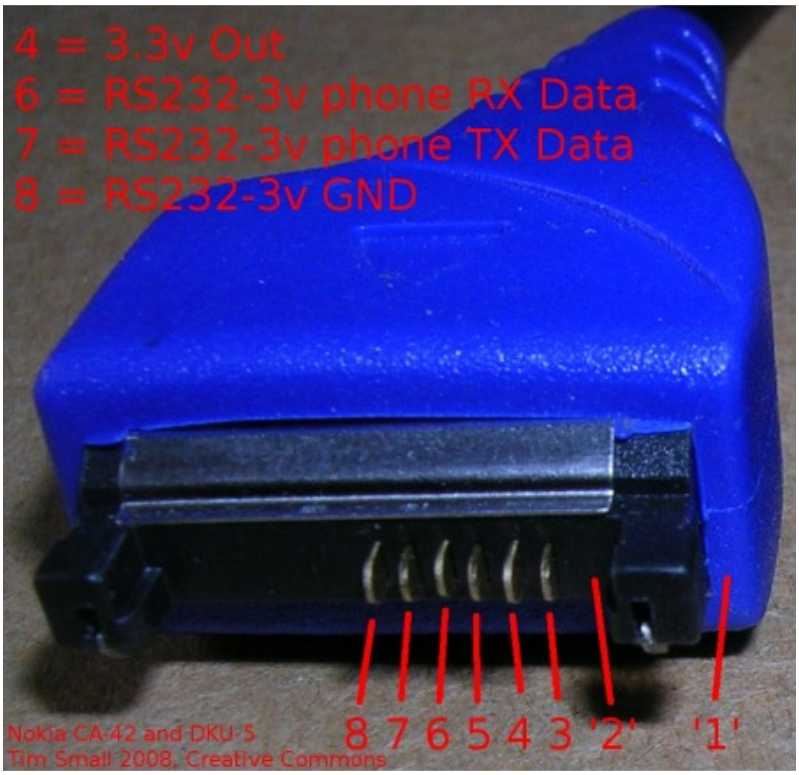


4 контактный разъем **serial** и 14 контактный разъем **JTAG**
(!оба не распаяны!)

Подготовка

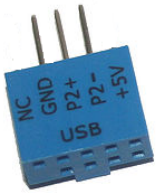
Для начала давайте подготовим все необходимое. Для прошивки понадобиться: кабель-адаптер USB-RS232 для подключения роутера к ПК через serial, патч-корд, TFTP сервер, терминальная программа, файлы прошивок.

Кабель. Нужен адаптер USB-RS232 с TTL 3.3v . к примеру, идеально подходит кабель для старых мобильников Nokia – CA-42. Он обладает всеми нужными нам качествами.



Кабель CA-42

Способ подключения приведен в таблице ниже. Как вы физически подключите кабель к разъему зависит только от вас. Можно просто припаять провода в нужней последовательности к разъему на плате, можно распаять разъем на плате роутера и подключаться уже к нему, можно припаять контактную площадку к кабелю и ее рукой прижимать к контактам serial. Я использовал Q-Connector. На котором оставил только три контакта.

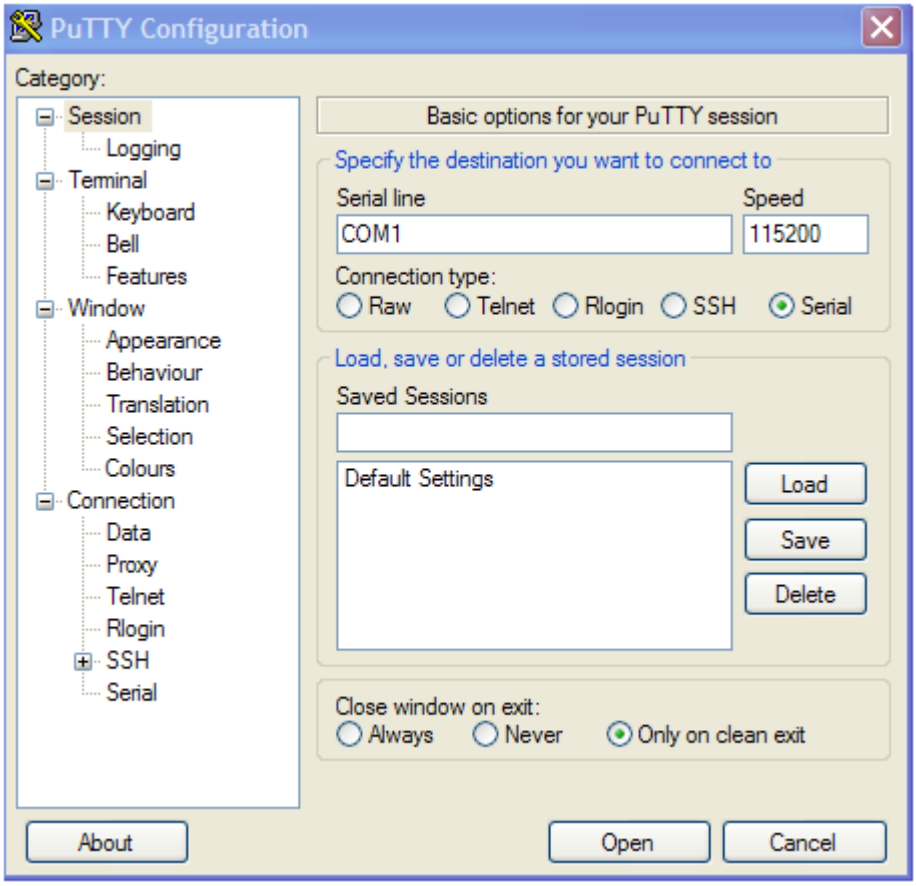


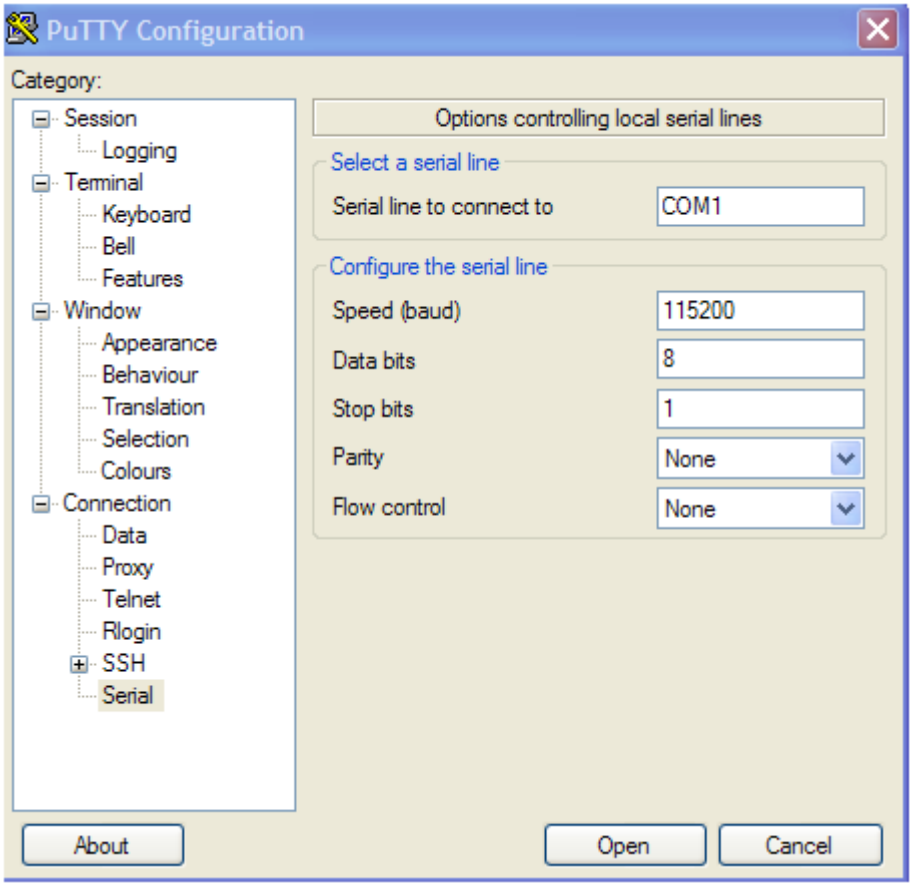
CA-42	Serial
GND	GND – pin2
Tx	Rx – pin 3
Rx	Tx – pin 4

TFTP сервер. На этом сервере будет лежать файл прошивки. Я использовал программу WinAgents TFTP Server 4. Качаете ее с сайта производителя и устанавливаете на ПК, к которому будете подключать роутер. Особых настроек она не требует. В каталог TFTP сервера (по умолчания для - C:\Documents and Settings\All Users\Application Data\WinAgents\TFTP Server 4\TFTPRoot\) ложем файл прошивки, который будем прошивать в роутер. ПК на который установлен TFTP Server должен иметь IP адрес 192.168.0.5 или 192.168.0.2. Это адреса по умолчанию для TFTP Server. Имейте виду что

на момент начала прошивки сервер должен быть запушен и в корневом каталоге должен лежать файл прошивки (*.bin).

Терминальная программа. Putty – отличная терминальная программа работающая через SSH, Telnet, rlogin и serial. Для правильного подключения через serial нужно сделать настройку как на картинках (разумеется, в место COM1 указать свой порт).





Файлы прошивок. Если вы будете прошивать в роутер сторонний софт Open-WRT или DD-WRT можете смело качать последнюю прошивку с их сайта и прошивать ее. Если вы сразу хотите прошить заводскую прошивку, то тут начинаются нюансы. Как пишут в Wiki на сайте Open-WRT для прошивки на заводскую прошивку нельзя выбирать файл прошивки в названии, которого присутствует слово «**boot**» к примеру, **wr1043nv1_en_3_9_17_up_boot(091118).bin**. При прошивке такого файла затрется бут и устройство будет полностью не рабочим. Надо выбирать прошивки с таким именем как на пример **wr1043nv1_en_3_11_5_up(100427).bin**. Я не стал рисковать и решил прошить прошивку Open-WRT, а потом с нее уже перепрошился на заводскую.

Разборка устройства

Теперь почти все готово для прошивки. Осталось его разобрать. **Помните, что разборка устройства лишает вас гарантии.** По этому делайте все как можно аккуратнее, не спеша, не оставляя следов.

- Переворачиваем устройство ножками к верху
- Аккуратно отклеиваем две задние ножки
- Откручиваем два шурупа соединяющие две части корпуса
- Откручиваем шайбы с выходов антенн
- Аккуратно вдавливаем выходы антенн внутрь корпуса
- Тянем на себя центральную часть корпуса (ребристую рамку). Надо приложить не большое усилие.
- По бокам на внутренней стороне лицевой части устройства отщелкиваем две защелки.
- Разделяем нижнюю и верхнюю часть корпуса.

Прошивка

- Подключаем кабель CA-42 к ПК и устанавливаем для него драйвера (идут в комплекте с кабелем).
- Другой конец кабеля подключаете к serial разъему роутера (можно подключать и во включенном и в выключенном состоянии).
- Соединяем роутер и ПК сетевым кабелем.
- Включаем роутер в розетку.
- Запускаем Putty и подключаемся к роутеру
  В окне Putty вы увидите примерно следующее:

```
AP83 (ar9100) U-boot 0.0.11
DRAM:
sri
32 MB
id read 0x100000ff
flash size 8MB, sector count = 128
Flash: 8 MB
Using default environment
----------------------------------
Autobooting in 1 seconds ...
```

И так будет повторяться раз за разом. Для того что бы роутер перестал перезагружаться в момент когда на экране появиться "**Autobooting in 1 seconds ...**" надо ввести на клавиатуре «**tpl**». Если вы успели то на экране появиться приглашение к воду команд, а сетевое подключение, не активное до этого, станет активным, индикаторы роутер перестанут мигать.

- Вводим первую команду и ждем пока не появиться новое приглашение к вводу команды.

  erase 0xbf020000 +7c0000

  где **7c0000** (8 126 464 байт в десятичной системе) это размер фала прошивки который вы будете прошивать в шестнадцатеричной системе. Обязательно учтите это! Перевести число из десятичной в шестнадцатеричной систему можно с помощью калькулятора встроенного в Windows.
- Вводим вторую команду и ждем пока не появиться новое приглашение к вводу команды.

  tftpboot 0x81000000 code.bin

  где **code.bin** это имя файла прошивки лежащего у вас на TFTP сервере.

- Вводим третью команду и ждем пока не появиться новое приглашение к вводу команды

  cp.b 0x81000000 0xbf020000 0x7c0000

- Вводим четвертую команду

  bootm 0xbf020000

  после того как на экране появятся строчки:

```
----------------------------------------
jffs2_scan_eraseblock(): End of filesystem marker found at 0x0
jffs2_build_filesystem(): unlocking the mtd device… done.
jffs2_build_filesystem(): erasing all blocks after the end marker… done.
mini_fo: using base directory: /
mini_fo: using storage directory: /overlay
```

  Надо перезагрузить роутер – обесточить его на несколько секунд.

Если все было сделано правильно и после включение устройство не продолжает мигать всеми индикаторами и сетевое подключение активно то через 30 – 60 секунд вы сможете зайти веб-интерфейс устройства.

Если вы сразу зашили заводскую прошивку, то можете дальше не читать, так как ваше устройство готово к работе. Если Open-WRT или DD-WRT то читаем дальше.

Перепрошивка с Open-WRT на заводскую прошивку.

Сейчас наше устройство работает, но на нем установлен «враждебный софт» Open-WRT или DD-WRT.

У меня стоял **Open-WRT**, поэтому начну с него.

- Запускаем Putty, вводим адрес 192.168.1.1, connection type SSH. При подключении у нас затребуют имя пользователя и пароль. По умолчанию root и 1234 соответственно. Имя пользователя и пароль можно изменить в веб-интерфейсе.
- Теперь необходимо закачать файл прошивки в память устройства с USB устройства или из сети/интернета. Я выбрал из сети. Для этого я запустил на своем ПК (ip 192.168.1.100) FTP сервер (запущенный ранее TFTP сервер не подойдет) и положил на него файл прошивки. При выборе прошивки я руководствовался рекомендацией приведенной выше и выбрал файл в имени, которого не было слова «boot».
- Поочередно вводим команды

cd tmp
wget ftp://192.168.1.100/tplink.bin
mtd -r write /tmp/tplink.bin firmware
reboot

Готово. После перезагрузки вы сможете зайти веб-интерфейс устройства и увидите родную заводскую прошивку.

Для **DD-WRT** могу рассказать в теории.
Для начало в веб-интерфейс DD-WRT надо включить поддержку USB и автоматическое монтирование устройства при его подключении. Перезагрузить роутер. Скачать по ссылке http://depositfiles.com/ru/files/orv90dbqt файл прошивки Подключиться к устройству через Putty и ввести следующие команды:

mtd -e linux -r write /mnt/<firmwarefilename.bin> linux

На экране появятся следующие надписи.

```
root@ router_name:/tmp# mtd -r write /mnt/<firmwarefilename.bin> linux
Unlocking linux ...
Writing from /mnt/0x20200.bin to linux ... [w], which the [w] will change
between [w] and [e]
```

После чего роутер перезагрузится.

Материалы, использованные мной при написании статьи:

http://wiki.openwrt.org/toh/tp-link/tl-wr1043nd

http://halfface.se/wiki/index.php/Openwrt

http://www.youtube.com/watch?v=9pumxmUyfuI

http://forum.ixbt.com/topic.cgi?id=14:51517

http://wiki.openwrt.org/oldwiki/openwrtdocs/customizing/hardware/serial_console

https://forum.openwrt.org/viewtopic.php?id=26103

http://samiux.blogspot.com/search/label/TP-Link%20TL-WR1043ND

Отдельная благодарность человеку с ником **LinkZ** форума forum.openwrt.org за ответы на вопросы, а также **Владимиру**, который своей непоколебимой рукой держал контакты кабеля прижатыми к serial разъему роутера пока я вводил команды.

Статью подготовил и оформил ELVEON (Антон), адрес для контактов elveon@ukrpost.net