Contents

Introduction

Routers that have a serial port can often be recovered by using a serial adapter. This is an alternative to Jtag.

You MUST have a working boot loader on the router to use serial commands. If your boot loader is corrupted, you MUST use jtag to recover. If your router does not have a jtag port, and your boot loader is toast, put the router on a shelf and wave to it occasionally.

Serial ports are normally a four or five pins on the router motherboard. Usually, you have to solder to pads or remove solder from the holes and install a four or five pin header.

Here is a link to some serial pinouts: Serial port pinouts

Some routers have serial ports inside the wan ports: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=62998

Redhawk0 summarized this information this way:

Serial cable is required to possibly debrick units without JTAG port. Serial cable can be either USB or DB9 connection type. It must be capable of doing voltage level shift to +3.3V not just +5V. There are 4 connections that are required for Serial to function properly. +3.3V, GND, Tx and Rx. Some boards are NOT marked with pin designation. You must use an OHM meter to determine both your power and GND in this case so things don't get connected backwards and blow out your cable chip. Then you can guess at the last 2 Rx and Tx lines. The cable has Rx and Tx but these are relative to the cable...so Rx line needs to be connected to the routers Tx line....because the router's designator's are relative to the router. So Tx and Rx get crossed for proper connection. On routers that have 2 Serial ports (Tx0, Tx1 and Rx0, Rx1) you generally use the zero port for your connections (I've not seen a router yet that you connect up to the "one" side) Once you make the connection setup your computer Serial terminal display for 115200 8-N-1. Plug in your router and you should see text on the screen. You can monitor the tty output of the boot loader as it is booting...or break in, usually by typing Cntl-C, and enter low level commands to try to fix things. The most useful for our purpose is the "nvram show" and "nvram erase" commands. Once the nvram is erased...type "reboot" or power cycle it....now tftp your firmware....or just let it boot up if firmware was previously loaded properly.

Hyperterminal and Putty

You connect to the router with the programs hyperterminal or putty.

The settings you want are: Baud: 115200 Data bits: 8 Stop Bits: 1 Parity: none No Flow control

On Windows XP:

Hyper terminal Setup In Windows XP, Click Start Button-->All Programs-->Accessories-->Communication-->HyperTerminal Enter a name for the connection, Click ok Choose com port you adapter is plugged into, Click ok Set: Bits per second = 115200 Data Bits = 8 Parity = none Stop bits = 1 Flow control = none Click ok Click File-->Save As, and select a place to save it to so you don't have to enter the settings again.

Putty Setup After installing putty, run it Serial line = The COM port your using for serial (ie. COM3) Speed = 115200 Click on Serial under Connection Serial line to connect to = same as above (Serial line) Speed (baud) = 115200 Data bits = 8 Stop bits = 1 Parity = None Flow control = None Click Session Enter a name for your connection under saved sessions Click Save Click Open

Serial Interfaces

You NEED a level shifting 3.3v TTL serial adapter. This is a special serial adapter. YOU CANNOT USE A SERIAL ADAPTER THAT IS NOT LEVEL SHIFTING! The Nokia CA-42 cable is a level shifting serial adapter. Other proper serial adapter are available from ebay and amazon and other online sources. You can get Nokia CA-42 cables online for about 3.00 and cut the phone end off. Then you have to figure out what each wire does. You need only grd, tx and rx connected properly for the serial interface to work. Tx on the adapter goes to rx on the router and rx on the adapter goes to tx on the router.

See this picture: You only need the wires connected to pins 8, 7, and 6 in this picture: (If no wire is connected to pin 8, the pin marked pin 2 in this picture should be ground instead)

http://www.dd-wrt.com/phpBB2/files/ca_42_dku_5_pinout_352.jpg

Here is what redhawk0 did: I cut the connector end off and found 3 wires. Blue, Red, and Orange.

Using an Ohm meter I determined that my Orange Wire is Ground.

Then using the "guess" method, I found the Blue wire gets connected to the router's Rx line and the Red wire gets connected to the router's Tx line.

When I plugged it into my XP rig...the cable was not recognized and no drivers found during the PnP process.

I downloaded a utility determining the attached hardware (UVCViewer):
http://www.users.on.net/~fzabkar/USB_IDs/UVCView.x86.exe

Then downloaded the Prolific Driver from here:
http://prolificusa.com/drivers/PL2303/PL2303_Prolific_DriverInstaller_v130.zip

And the updated 1.4.17 driver which supposedly provides better support for Vista/Win7 Machines: http://prolificusa.com/drivers/PL2303/PL2303_Prolific_DriverInstaller_v1417.zip

So...

Orange = GND Blue = Rx Red = Tx

Once loaded and connected...my laptop sees the unit attached to COM8....configured Putty....and all is well.

LOM stated:

No there is no fixed standard for the colours of the wires and obviously not on the number of wires either. My first CA-42 had 3 wires and the ones I bought later had 5, the picture in my post above is from one of those.You can carefully remove the plastic molding of the phone connector and see where each wire is going and find out which colour the respective signals are on. Schematic of the Nokia phone connector here: http://www.hardwarebook.info/Pop-Port

strfr stated: The "level shifting 3.3v TTL adapter" is must, you can't connect router straight to standard RS232 serial interface. Learned after hours of trying.. ;] Cheap CA-42 is all right, even the chinese clone with ARK3116 chip thus you will not find proper driver for Win7 64bit system. Windows XP mode is the solutions in such a case.

Malachi stated:

I have purchased a few of the Nokia clones that didn't work, for that reason I buy USB to uart adapters like these http://www.dx.com/p/usb-to-uart-5-pin-cp2102-module-serial-converter-81872#.VqrGiEo8KK0

Serial Commands

You have less than a second to stop the boot so that you can enter commands from the serial prompt. You do this by hitting cntl-c JUST as the router is starting up. If it goes too far, you will not be able to stop it. Get someone to start the router while you are hooked up and madly hitting control-c. If the scroll lock key is on or if flow control is set to anything but off or none, you can not stop the boot.

Erase Nvram

Power cycle the router and while it is booting hit control C quickly just as your router starts You should get a CFE> prompt

The most common command you will use is the "nvram erase" command. This command will erase the nvram values that are often the cause of bricked routers

At the cfe prompt:

```
cfe> nvram erase [enter]
```

To flash the firmware

This assumes you have a ttl adapter connected and ready to go. There is reference to stock firmware. This does not apply to router that used to run vxworks. All of those, have jtag tmk..

connect that bitch (the router to your serial adapter).. 115200,8,1,n and no flow control are the com, param's

I use hyperterminal. In the terminal, boot the router.

Immediately start hitting ctrl-c. If you hit it right you will be at the cfe prompt:

```
cfe>
```

Execute the **nvram erase** command at the CFE prompt

Get the tftp utility ready to flash the STOCK firmware for your router so all you need to do is hit enter to launch.

You are going to tell the router to accept a tftp flash of firmware. It times out quickly so that is why you need to get the utility ready to launch.

Static ip on your rig.. 192.168.1.10, mask 255.255.255.0, not necessary but gateway 192.168.1.1

If you have a linksyse router, at the cfe prompt:

```
flash -ctheader : flash1.trx
```

For other routers try:

```
flash -noheader : flash1.trx
```

hit enter.. the router will want an upload of the firmware. It will time out after three tries. Don't let it time out, now launch the tftp utility. It will upload, program and then you will be back at the cfe prompt. This will take some time. You will see what is happening in the console.

You will be back at the cfe prompt when it is done:

```
cfe>
```

issue a "go" command:

```
go [enter]
```

the router will launch its new firmware.

Let it boot. It will boot 2 ~ 3 times.. You are done.

Now install dd-wrt again.

Good Luck..

Barryware's Detailed Instructions for Linksys

Start banging ctrl-c at the same time you power up the router. If successful, you will be at the cfe prompt: cfe> have your tftp utility all que'd up to flash the STOCK LINKSYS firmware for your router. Make sure you have a static ip on your rig.. The router will not have the dhcp server running. At the cfe prompt type:

```
nvram erase [enter] ([enter] means hit the enter key Wink )
```

a couple of seconds later, you will get a command status = 0.. that is good. You will be back at the cfe prompt. Now type:

```
flash -ctheader : flash1.trx [enter]
```

(note the space before & after the colon) Now immediately launch the tftp utility on your computer. The router will listen 3 times, after that it will time out so you gotta be fast. You will see that it is programming.. this will take a bit of time. When it is done, you will again be back at the cfe prompt. After the flash chip is programmed and you are back at the cfe prompt, either power cycle the router (I prefer) or type:

```
go [enter]
```

the router will boot three times. then you are good to go with stock firmware. From there, install dd-wrt again following the normal procedures. Have fun.. Good luck

One more time, for those who need repetitive instructions:

1. serial is to communicate with the router and issue the commands.
2. All data to flash goes through the lan ports.
3. Stop the boot via ctrl-c (You have to be faster than humanly possible to hit ctrl-c fast enough!)
4. tell it to accept a tftp upload of the firmware (through the lan port(s) (eth0)) by issuing the command: flash -ctheader : flash1.trx [enter] ([enter] = hit the enter key)
5. then immediately launch the tftp utility on your computer and send the proper firmware to the router. It times out fast so issue the command, launch the utility.
6. Flash stock linksys firmware when debricking a router. (You can flash dd-wrt again, following the wiki instructions for your model of router.

when back at the cfe prompt:

```
nvram erase [enter]
reboot [enter]
```

the router will boot 3 times. Don't be scared.

LOM has stated this for the E3000:

The easiest way of flashing an E3000 when you have serial terminal attached is:

```
nvram set safe_mode_upgrade=on
nvram commit
```

```
reboot
```

now connect with your browser to 192.168.1.1 which will bring up the CFE recovery gui page where you can upload the firmware.

Troubleshooting

Some (not all) usb ttl converts need vcc connected.. Some only tx, rx, and ground.

If you are unable to write data to.flash chip.due to.a.bad boot.block, try writing.to.another location. This should be done.with caution.as a last.resort: Look for "Boot partition size =" at the cfe boot.

this was listed at the cfe boot just under intiallizing arena services on my router and is where you get the address location from for the flash command.

Boot partition size = 262144(0x40000)

```
flash -offset=262144 -noheader 192.168.2.10:dd-wrt.v24_micro_generic.bin flash0
```

Just for your info 192.168.2.10 was my windows pc hosting the firmware via a tftp server.

What the commands above basically do is tell the cfe to flash the firmware at a particular address location on the flash chip instead of the location that the cfe thinks is the correct one which obviously is not since your getting a bad boot block

If you are receiving no output, remove the tx & rx wires from the router and twist them together. Open a terminal session and type on the keyboard to see if your typed characters are echo'd correctly in your terminal. If you see what you typed, the COMPUTER is set up properly. So look to your connection to the router as the source of your problem.

If you still don't see output, the problem is with your computer setup. Check your com parameters. Depending on the hardware & driver, you may have to set the parameters in the device manager as well as your terminal software.

Garbage characters on the screen usually is a bad connection, especially a bad ground. Check your connections with a multimeter.

If you cannot get a cfe prompt it is usually due to not being fast enough. Get someone to assist in turning on the router while you hit control c over and over again as fast as superman or Barryware. If that doesn't work try reversing the tx and rx to make sure that you are actually transmitting the command.

Links

Serial Thread in the Broadcom Forum: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=56739