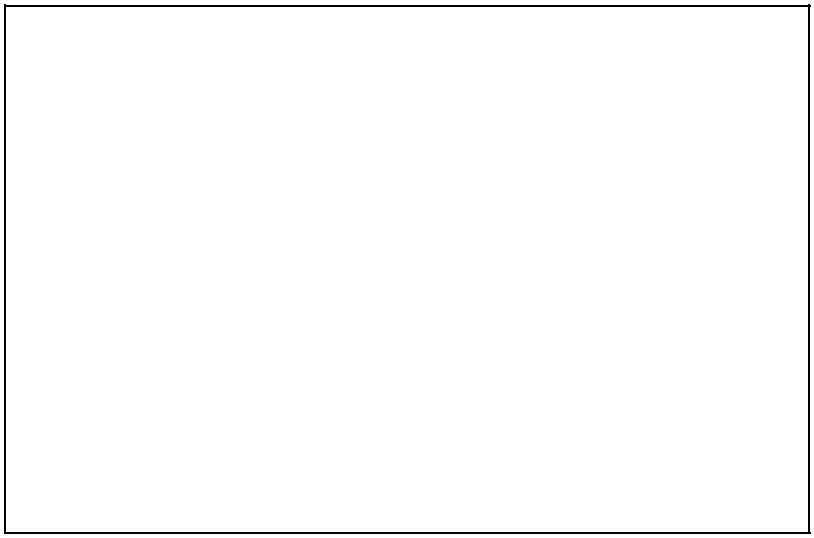
Contents

Hardware



The DIR-330 is an easy-to-deploy wireless VPN router solution designed specifically for the Small Office/Home Office (SOHO) market that demands superior performance and security.

Specifications

- CPU : Broadcom BCM5836PKPBG
- Flash Memory Chip: S29GL064A90TFIR3 SPANSION
- Flash Size: 8 Mb
- RAM: 32 Mb
- Ports: 4x 10/100 switch 1x 10/100 WAN
- Antenna: 2x RP-SMA
- Other: 1x USB 1.1 (According to tech specs on Manufacturer page. Port Inactive according to manual)

- Hardware Rev: A1 (only tested on this hardware rev. - please update if you have another rev.)

D-Link DIR-330

Major Edit: 2/10/2010 mpf - Thank you to DarkShadow for starting this Wiki. I am sure he knows how much work is involved with typing tutorials. Originally, there was much information on the DIR-320. Because that router is such a different animal, I deleted all references to it to avoid confusion. The info now in the wiki is exclusive to the DIR-330. I have tried to address all of the topics that were present on the DIR-320 to ensure that none of the small suggestions were lost.
I would strongly suggest if you are looking to install DD-WRT then read this wiki from beginning to end. Make sure you fully understand what is involved. It is very hard to write procedures that cater to both experienced and novice users. Hopefully there is some balance here, but wiki's are generally geared toward the novice. Step by step instructions are given, but the commands specific to the OS used are not discussed. If you are not familiar with basic commands like ping, telnet, tftp, etc. learn them before you try to install DD-WRT. I honestly do not want to start a debate about which OS to use, but I will offer some suggestions based on my experience writing and testing this wiki. Windows (tested w/XP 32 bit) or Linux (tested w/Ubuntu 9.10 32 bit) can be used for installing firmware, but I would strongly recommend Linux for JTAGing. I did use Windows for some JTAG testing, but the Ubuntu 32 bit 9.10 Live CD proved to be a much more solid environment. That really should not be a suprise to anyone who understands OSs and how they are built. I chose the Live CD because many people may not have Linux installed as a base; this way, anyone can use a Linux environment for a short period of time and have a positive result. Consult the Ubuntu website for how to download, create and use that disk.
Of course, it goes without saying that if anyone finds an error or the procedure needs to be updated please do so.
All testing in this wiki was with Broadcom Generic versions of Brainslayer v24 preSP2 (Build13525)
ht

DD-WRT, OEM & Other Information

Official D-Link homepage for the product. Here you find the manual as well as the stock firmware releases:
Click here

DD-WRT firmware used during testing of this Wiki:
Click here (not recommended, very old)
There is a file named DIR330 in the directory, it is identical to Mega Generic version. So, either file may be used. See Where do I download firmware? for links to newer builds.

Peacock Thread refered to in many places: Click here

JTAG software version 2-1-4 used for all testing: Click here

Direct link to the CFE and NVRAM that you will need for JTAG support: Click here

OpenWRT wiki page for the Dir-330:
Click here

Forum Threads

Large thread regarding the debricking of the device. JTAG pin outs in the pics of the next section.
Click here

Pictures of Hardware

Picture of the PCB hardware release A1 - here with JTAG Pin identification:
Click here

Universal JTAG cable and instructions:
JTAG cable
Instructional JTAG wiki

Flashing to DD-WRT

How to Install DD-WRT from the DLink OEM screen on firmware 1.12:

1. Download the Generic Broadcom Mini version and the Mega version if you want to install that as well. Do not try to install the Mega version directly. Testing showed repeated mixed results including two bricks. Testing always succeeded with Mini installed first. Rename the MINI file to start with 'dir330'. OK to rename the MINI file to just dir330.bin; again, filename must just start with 'dir330'.
2. If you own a JTAG cable, download version 2-1-4 of tjtag as well just in case things go really astray.
3. Make sure your computer is the only device connected to the router. Port 1 was always connected to for testing.
4. Do a factory reset on the box. Ref Peacock thread. Router should return to DLink factory setting of **192.168.0.1**
5. Set your PCs static ip to 192.168.0.25, net mask 255.255.255.0, def gateway 192.168.0.1
6. Open a web browser (tested with Firefox 3.6 and IE8)- clear cache, cookies, etc.
7. Type in 192.168.0.1 in the web browser
8. Login default should be username 'admin'leave password blank
9. Navigate on DLink pages to Maintenance on the top, then Firmware on the right.
10. Click <check now> for the latest firmware- wait for this to fail. If you do not do this worthless step, you will receive a file name error on the next step. (So I guess it has some worth?)
11. Browse to the renamed DD-WRT MINI firmware file on the webpage - remember, this filename must be renamed to start with 'dir330'.
12. Click <apply>
13. Answer 'OK' on the popup box
14. Wait for 2 mins 10 secs and the router will start flashing the blue light. Eventually, the web browser may say the firmware upgrade is complete and to click continue. Do NOT click the continue button, just move on to the next step.
15. Set your PCs static ip to 192.168.1.25, net mask 255.255.255.0, def gateway 192.168.1.1
16. Leaving browser window open, then open a terminal or command window.
17. Try to ping 192.168.1.1
18. After a good ping, telnet into 192.168.1.1
19. User name is always 'root' password is 'admin'
20. At the '#' prompt, type 'erase nvram' hit <enter>

21. At the '#' prompt, type 'exit' hit <enter>
22. Cycle power on the router
23. You will see the blue light flash and come on for about 30 seconds, flash again then go off. this is the process of initializing the router and NVRAM.
24. Once stable (about 1 min), cycle power on the router again.
25. You should now see the blue light flash and come on for only about 8 seconds.
26. You should be able to go back to the browser and type in 192.168.1.1 and see the password reset screen. Enter username and password info as required.
27. DD-WRT MINI is now installed. Proceed on to install the MEGA version

Continue on for MEGA install:

1. Navigate on DD-WRT page to Administration - Firmware Upgrade
2. Browse for the MEGA firmware file you wish to install.
3. Click <Upgrade>
4. Wait, watch and do not touch your system; nothing looks like it is happening for a VERY long time. The screen says 'Wait', and they mean it.
5. The webpage will count down then stop. It seems like it may even be hanging. Just wait.
6. At 9 minutes 30 seconds in, the blue light on the right of the box should come on. At 10 mins, the blue light should be out, and the web page should reload to the Basic Setup Screen. If after 12 minutes you do not see the blue light flash, you can start over, or go to the flash recovery section.
7. Technically, you are done. But, erase the NVRAM again just to ensure total success and normal operations.
8. In the command/terminal window, you should be able to ping 192.168.1.1
9. After a good ping, telnet into 192.168.1.1
10. User name is always 'root', the password is what you set it to at the end of the MINI install.
11. At the '#' prompt, type 'erase nvram' hit <enter>
12. At the '#' prompt, type 'exit' hit <enter>
13. Cycle power on the router
14. You will see the blue light flash and come on for about 30 seconds, flash again then go off. This is the process of initializing the router and NVRAM.
15. Once stable (about 1 min), cycle power on the router again.
16. You should now see the blue light flash and come on for only about 8 seconds.
17. You should be able to go back to the browser and type in 192.168.1.1 and see the password reset screen. Enter info as required.
18. DD-WRT MEGA is now installed and you shall forever be happy.

Flashing Back to D-Link Firmware

With DD-WRT installed (tested with mini and mega), to go back to D-Link firmware:

1. Do a hardware (push the button) reset to return to defaults. Ref Peacock thread. Router should return to **192.168.1.1**
2. Set your PCs static ip to 192.168.1.25, net mask 255.255.255.0, def gateway 192.168.1.1
3. Open a web browser (tested with Firefox 3.6 and IE8)- clear cache, cookies etc.
4. Type in 192.168.1.1 in the web browser
5. During login, you should set username and password (make them simple) - if not, the hardware reset did not take. Reference the Peacock thread and start over.

6. Navigate on DD-WRT page to Administration - Firmware Upgrade, then leave browser window open on this page
7. Open a terminal or command window.
8. Telnet into the router - 192.168.1.1
9. User name is always 'root' (no matter what you set above), password is what was just setup on the web login
10. At the '#' prompt, type 'erase nvram' hit <enter>
11. At the '#' prompt, type 'exit' hit <enter>
12. Do not close terminal/command window, move back to the browser
13. Leave 'after flashing, reset to' box set to "Don't reset"
14. Browse for the DLink firmware (currently 1.12) you wish to install
15. Click <Upgrade>
16. Wait, watch and do not touch your system; nothing looks like it is happening for a VERY long time. Your patience will be tested.
17. The webpage will count down then stop. It seems like it may even be hanging. Just wait.
18. At 8 minutes in, the blue light on the right of the box should come on; at 8 mins 30 seconds, the status light should start blinking. Move on to the next step. If after 10-12 minutes you do not see the blue light flash, you can start over, or go to the flash recovery section.
19. Do NOT power down yet; unpredictable results may happen. In the command/terminal window, you should still be able to ping 192.168.1.1
20. If you can't ping the router, it either worked or you will need to recover. Skip down to step 25 to test if it accidently worked.
21. If you can ping the router on 192.168.1.1, telnet into 192.168.1.1
22. It may hang with no response and there will be no username/pwd prompts. just hit <enter> a few times
23. Type 'erase nvram', hit <enter>, type 'exit', hit <enter>
24. Power down the router for 5-10 seconds. Power up the router.
25. Once the router is back up after 30 seconds, you should no longer be able to ping 192.168.1.1
26. Set your PCs ip to 192.168.0.25, net mask 255.255.255.0, def gateway 192.168.0.1
27. Ping test 192.168.0.1
28. Type in 192.168.0.1 on the browser; login default should be username 'admin' leave password blank
29. Should see the default D-Link screen and then that makes you remember why you went to DD-WRT in the first place!

Bad Flash Recovery

OK, something went wrong with downloading firmware into the DIR-330. Now when you turn on the power, the only lights that come on are the power LED and the Port LED number you are wired to. Don't panic yet. This procedure may be able to take you to DD-WRT Mega.

1. Set your PCs static ip to 192.168.0.25, net mask 255.255.255.0, def gateway 192.168.0.1
2. Open a terminal or command window.
3. Try to ping address - **192.168.0.2** -- If you are NOT successful and there is no response, try to reboot/reset with hardware button. Still no success or changes? Proceed to JTAG section.
4. If you can ping **192.168.0.2**, you should be able to tftp firmware back into the box. The CFE on this router is waiting on 192.168.0.2 for a firmware upload. Do not waste your time with the emergency reload on 192.168.0.1 web page. Not only may it not work, it may leave you with only JTAGing as an option.

5. Decide what you want to install- this tutorial uses DD-WRT Broadcom Generic Mega. Filenames are not critical right now. Suggestions for firmware are either mini, mega or OEM builds. If the OEM build is going to be attempted, see the section on installing the OEM software back into the router. You may need to perform the steps to clear the NVRAM. This procedure is slightly different than with DD-WRT.
6. You should be able to tftp in a binary transfer mode to address 192.168.0.2 with your firmware. A tftp Windows XP example would be:

   ```
   tftp -i 192.168.0.2 PUT dd-wrt.v24_mega_generic.bin
   ```

   *adjust for another OS or filename accordingly. Your mileage may vary.
7. Within 30 seconds it should state that the transfer was successful
8. WAIT a total of about 3 mins 30 seconds and the blue light should start flashing.
9. Set your PCs static ip to 192.168.1.25, net mask 255.255.255.0, def gateway 192.168.1.1
10. Try to ping 192.168.1.1
11. After a good ping, telnet into 192.168.1.1
12. User name is always 'root' password is 'admin'
13. At the '#' prompt, type 'erase nvram' hit <enter>
14. At the '#' prompt, type 'exit' hit <enter>
15. Cycle power on the router
16. You will see the blue light flash and come on for about 30 seconds, flash again then go off. this is the process of initializing the router and NVRAM.
17. Once stable (about 1 min), cycle power on the router again.
18. You should now see the blue light flash and come on for only about 8 seconds. Life is good again.
19. You should be able to open a browser and go to 192.168.1.1 and see the password reset screen. Enter info as required.
20. When the system info screen comes up, verify your MAC has not been corrupted. Your LAN MAC should be one less than the MAC on the bottom of the case. Wireless MAC one more than the MAC on the bottom of the case. It will be obvious because the MAC will be completely different than what is on the bottom of your router.

JTAG Information

The JTAG process should not be feared, but it most certainly should be respected. You will be working with open unprotected circuit cards, so proper precautions should be maintained with regards to ESDS. If you have never done a chip level type programming, there are some outstanding wiki's about the subject. JTAG wiki One the great things about this website is the unbelievable wealth of information that is available. Again, if you are new to this, spend some time reading.

There are probably a few configurations that will work for the JTAG setup. What will be discussed here will be a very solid and repeatable setup that worked well for me.

In order to JTAG your router, you will need to either build or purchase a JTAG cable. Tornado recommends the Universal JTAG cable which is listed in his signature on the forum boards and up top in the Pictures section. My own experience with it has been very positive. It can be used in several configurations. I found it to be very solid in performance.

The most difficult part about the JTAG process is that it requires a header on J4 be soldered into the router board. Reference the Pics section above. This can be tricky if you have never performed this type of

desoldering and soldering before. Solder needs to be removed from the holes before pins are inserted or a header strip is inserted. I am not going to go into any detail about this, but if you do not know how easy Electro Static Discharge damage can occur you should not be attempting this step.

As mentioned above, Ubuntu 9.10 32bit Live CD was used for all my testing and recovering. I did some testing with Windows XP, but found this platform not as repeatable as Linux.

Up in the information section, there is a link to download the CFE and NVRAM for the DIR-330. You will need both of these in order to JTAG the box. Read and follow the instructions in the post to modify the NVRAM file to include your MAC address. The CFE for this unit looks for the MAC in NVRAM on boot up. The MAC info is right at the beginning of the NVRAM file and the specifics of how to modify it are in the post.

The following steps should help in achieving your goal:

1. Plug the router's power cube into a power strip which contains a switch if you have one. Most power strips have switches built in these days. Configure it so that you have easy access to the switch and the keyboard of the computer you will be working with. You may need to issue commands quickly on power up.
2. Do not power up the router at this time. Do not plug any cords into the router other than from the JTAG cable. Do not plug the JTAG cable into the computer/laptop. Do not connect the USB port to the JTAG cable (this is for the universal board listed in the Pictures Section above).
3. Using the pictures of the DIR-330 A1 board in the Pictures Section above, connect only to the following pins: nTRST (pin 1), TDI (pin 3), TDO (pin 5), TMS (pin 7), TCK (pin 9) and Ground (pin 2). Use the instructionshttp://wiki.dd-wrt.com/wiki for the Universal JTAG board listed above configured for **Buffered** mode. Triple check your connections.
4. Ensure that the TJTAG program, the CFE and the modified NVRAM are located in a directory you can access once the Live CD is booted. This can be locally or on a network drive. You just need to know what directory you are using. The CFE and NVRAM must be named CFE.BIN and NVRAM.BIN and be located in the exact same directory as the tjtag linux program. Commands concerning file names are case sensitive under Linux.
5. Boot up the Ubuntu Live CD.
6. Open a terminal window.
7. Type 'sudo rmmod lp' hit <enter>
8. navigate to the directory containing the Linux version of the tjtag and the CFE/NVRAM files.
9. connect the JTAG cable to the computer.
10. connect the mini USB cable on the JTAG board to an open USB port. This is just to supply power to the buffer chip. The light should come on the JTAG board.
11. power on the router
12. at the prompt, type "sudo ./tjtagv2 -probeonly /wiggler" hit <enter>. Give it several seconds if it does not complete right away.

If you were successful, it should have completed immediately and said "*** REQUESTED OPERATION IS COMPLETE ***". The information should show that the processor (Broadcom BCM4704 KPBG Rev 9 CPU chip) and the Flash chip were detected and that the processor entered DEBUG mode. Let's assume that happened and press on...

1. Use the up arrow key to recall the previous command -"sudo ./tjtagv2 -probeonly /wiggler" hit <enter>. You should get the same results. Wait a few seconds and do it again. If it is responding every time, then you can proceed with the next steps.

2. It has been recommended that the CFE and NVRAM be backed up and saved. You should do this at least three times to ensure that the setup is working properly.
3. The commands are: "sudo ./tjtagv2 -backup:cfe /wiggler /bypass /silent" and "sudo ./tjtagv2 -backup:nvram /wiggler /bypass /silent". Every time you issue this command, it will write a new file with a unique timestamp in the tjtag directory.
4. If the downloaded CFE files all match, and the downloaded NVRAM files all match, then you can proceed on confidently.
5. You can compare the CFE files you downloaded to the one you pulled from the link above in the Information Section. If they match, no need to flash the CFE. The NVRAM will not match, but you should see your MAC in the files you downloaded unless it was corrupted.
6. From here, you will upload the CFE (if needed) and modified NVRAM with the following commands:"sudo ./tjtagv2 -flash:cfe /wiggler /bypass /silent" and "sudo ./tjtagv2 -flash:nvram /wiggler /bypass /silent"
7. Now if things are going really well, just issue the following command: "sudo ./tjtagv2 -erase:kernel /wiggler /bypass /silent"
8. You should now be able to proceed to Bad Flash Recovery section above. Before you do, power down the router, unplug the USB cable and then pull the JTAG board off of the PC.

OK, now let's spend some time working on if you did not detect the CPU or Flash chip. If you did not detect the CPU, go back over the procedure and recheck all of your connections. You can have some wires misplaced and still grab the CPU. The CPU was always detected even if it would not enter debug mode. If you cannot detect the CPU, well... :(

1. If you detected the CPU (Broadcom BCM4704 KPBG Rev 9 CPU chip) but it was 'hanging' on the flash detection or some other area try the following: Turn of the router. Prepare the command "sudo ./tjtagv2 -probeonly /wiggler" but do not hit enter. Power up the router and then hit enter. If it hangs, immediately hit <ctrl>'c' to kill it, up arrow to recall the command and hit <enter> again. Repeat again and again as fast as possible for 10-15 seconds.
2. If the probe command finished properly and detected the chip during one of those attempts, then you will be able to recover by using this technique to erase the corrupted memory. If there is no detection, recheck you connections and try cycling the power on the router and try this process again.
3. If after doing this a few times, it may seem like there is a small window for you to 'catch' it in for it to work. Repeat the process but now use the following command: "sudo ./tjtagv2 -erase:wholeflash /wiggler /bypass /silent". Again, same as before. On power up, if it does not start working right away, <ctrl>'c' out of it and resend the command. You may even want to try doing this while holding in the reset button on power up. Eventually, the command will take and it will erase the whole flash.
4. Once the whole flash is erased, cycle power on the router and download the CFE and NVRAM as described above. Check communications first with the probe command.
5. You should now be able to proceed to Bad Flash Recovery section above. Before you do, power down the router, unplug the USB cable and then pull the JTAG board off of the PC.

Final closing thought on JTAGing; do not try to force detect the memory if you can 'see' the CPU but not the Flash on a probe. If tjtag is having trouble 'talking' to the CPU, then the CPU is trying to do something else. During the testing it did not seem helpful to force chip detection. Forcing chip detection on erase or writes made it look like it was doing the process when it actually was not.

Random Notes

1. When flashing, do not power down unless explicitly told to do so.

2. Pay close attention to the IP numbers referenced in various places. They can be different than other routers, especially during firmware recovery.
3. Read each section completely before you begin.
4. Be patient; use a stopwatch. Time seems to almost stop while you are waiting to find out if a firmware flash worked.
5. Make sure you tell your wife & kids to leave you alone while you flash your router. You do not want to let them see you sweat over something so small and ridiculous.

User Comments

Edit 2/11/2010 - Corrected for the actual files used for the testing. mpf

Words for the Search engine

DIR330, DIR-330