Alternative Firmwares for your Router

AKA - Fix your F***ng Router Already

by Aaron Grothe

Disclaimer

We're going to be talking about flashing and making changes to your router.

Replacing the firmware on your router can/probably will invalidate your warranty and in a worst case scenario give you a very poor night light instead of a router.

Introduction

For a lot of routers you have a choice of firmware. There are several alternative firmwares available for quite a few routers.

We'll talk about a few of them tonight.

Introduction

Couple of Quick Questions:

How many of you are running the stock firmware on your router?
How many of you have updated the firmware on your router since you installed it?

Introduction (Continued)

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

Why Alternative Firmware?

- You're able to do things that the original manufacturers might not have intended with the router
  - Repeaters/Bridges/Mesh, etc
  - Increase/Reduce transmit power for device
  - VPN, EOIP, SSH access
  - Continued security patches/updates
  - Install adblocker/child safety software at the router to make it harder to bypass
  - IPV6 support and transitioning support
  - Want to run bittorrents off your router
  - Because you can :-)
  - Many more

Linksys WRT54GL

Released in 2005. Linksys flipped the firmware to Linux from VxWorks starting with version 5.

Cisco was sued by the GPL for initially not releasing the code. The case was settled and people began to play with the code and created alternative firmwares for the router.

People have continued to modify/create alternative firmwares for their routers since this time.

Major Alternative Firmwares

DD-WRT
OpenWRT
LibreCMC
TomatoWRT

Bunch of others exist as well

DD-WRT

DD comes from the license plate prefix for Dresden where the initial development team lives. WRT - comes from the Cisco router.

DD-WRT supports a lot of hardware. The best resource is to hit the router database at

http://dd-wrt.com/support/router-database

Also recommend reading at their wiki

DD-WRT

Is actually the default firmware shipped with some routers such as Buffalo Networking products

Linksys has alternative dd-wrt software available for most of their routers.

MyOpenRouter has the Kong Firmware for a bunch of netgear devices.

DD-WRT

DD-WRT is my usual go to distribution. I know the interface pretty well and it works pretty well on most hardware

DD-WRT also has Optware packages which makes a lot of additional packages available to install on your router.

DD-WRT Example #1

- My parents house has a ASUS 1300AC router in the den it is a pretty good router. Currently running dd-wrt on it.
- Downstairs is an LG plasma TV. One of the last of the plasmas. Works pretty well except for the networking. It continually drops the 5ghz connection and it forces you to reenter the PSK every time
- Took an older router a Linksys n600 I believe. Put dd-wrt onto it. Set it up as a bridged router and use the wired connection from the tv to the local router
- No more drops or putting in the PSK all the time.

DD-WRT Example #2

My current DD-WRT setup. Have a Nighthawk router. Ran DD-WRT on it for some time. Could not get consistent 5ghz access on it. Have reverted to the stock firmware for the time being. Have had to accept some limitations in the stock firmware. E.g. Doesn't do DNS reservations the way I like. E.g. I do a dhcp request from my debian box named debian. The stock firmware doesn't answer dns requests for the name. Have had to delegate DHCP on my home network to my server. Continue to monitor Kong firmwares to see if one of them fix the issue.

Moral: Not always a success, but hopefully you can get back to stock.

DD-WRT Example #2b

Do have a TP-Link 841n setup which has a couple of SSIDs which I use to hook up devices I want to keep segregated from the rest of my network. It works quite well for that purpose.

It is locked down by iptables rules as well on the router so it doesn't try to talk to the rest of my network.

OpenWRT

- OpenWRT is a smaller distribution than dd-wrt. It isn't only used in routers. It is used in some small hardware as well such as the Ben NanoNote and some laptops. You can also run OpenWRT on an x86 desktop as well.
- One of the cool things about it is the buildroot system which is used to automatically build it from source.
- Uses opkg package format and has a lot of additional packages available for it as well. Python is available which means you can do SCAPY on it :-)

OpenWRT

Just bought a cheap router a couple of weeks ago and it came with OpenWRT on it. We'll take a look at it in a bit.

LibreCMC

LibreCMC is a fork of OpenWRT that is FSF-approved. This means it doesn't have binary blobs and the source for everything is available. This does mean it supports less hardware.

Tomato

Is another firmware that is available. Is a fork of the HyperWRT firmware.

Is partially opensource. The GUI is under a more restrictive license.

Doesn't support a lot of hardware.

Emphasis is on stability it doesn't reboot very often.

Can I use new Firmware?

Take a look at your router model number. Including the revision.

One of the most popular routers to play with is the TP-Link 841n(d). It is cheap around $20.00 on amazon supports both OpenWRT and DD-WRT for most revisions.

TP-Link recently release 841n v.13. This uses a new mediatek processor and it no longer works so make sure you research this quite a bit. This will hopefully change in the future.

Can I use new Firmware? (cont'd)

Recommend checking database on both OpenWRT and DD-WRT. Depending on what you want to do with them it will help make your choice. If you're just looking for a router I recommend DD-WRT if you're looking to turn your router into a computer I would consider OpenWRT. Both are very good.

See if your manufacturer has an official port of OpenWRT or DD-WRT or an "unoffical" one like Kong. This can be quite useful.

How do I flash my router?

Nowadays for most routers it is as simple as using the firmware update command in your gui to load a mini version of the new firmware. Then after that you can load the full version of the new firmware.

It isn't this easy on all routers. E.g. there is a very nice ASUS router that is sold as a T-Mobile cell hotspot. It goes on sale on slickdeals from time to time. To be able to put DD-WRT on it you have to do a bunch of commands to reformat the flash to be able to fit dd-wrt on there.

How do I flash my router?

Many years ago when I first did this on a netgear n600. I had to use telnet and a bunch of nvram commands to do this. Problem was I was using a mac for the serial connections and getting in the time window to interrupt the boot to get control was very fragile.

You kids don't know how well you have it nowadays with your ipods and your gigabit ethernet.

Let's flash a router

Let's flash a TP-Link 841n I've got

Right now it is running the stock firmware
I've already downloaded the correct firmware for it
Should be able to do just do it through the GUI

Bricking Note

I managed to brick one of these a couple of years ago by putting the wrong firmware on it.

I was able to recover it by using a tftp boot server and having it pick up the stock firmware that way

I could also open it up and connect a usb-serial adapter to internal pins on it. Since the tp-link supported a serial connection. Not all routers do.

30-30-30 Rule

In docs you'll see references to 30-30-30. 30-30-30 is quite simply.

- Hold down the reset button for 30 seconds
- Unplug the unit, continue to hold the reset for 30 seconds
- Plug it back in and continue to hold the reset button for 30 seconds

Will reset dd-wrt to defaults including for password :-)

For some routers (asus) you just do the first 2 steps

Demo

- Let's do it

Let's try out the OpenWRT router

Time to plug in the travel router and see how OpenWRT looks :-)

5 Tips for Success

1. Read the Wiki for your router
2. Read the Wiki for your router
3. Download the stock firmware from the manufacturer as well. Ideally current version as well as latest
4. Consider trying it on another/less important router before doing it on your main router
5. Know how to reset to the default firmware

One Killer Feature (Needed)

- Most of you know about my love-hate relationship with my portal router. It was my main router before I flipped back to the nighthawk.
- It has one amazing feature if you are in a place that is jammed with 5ghz it will use alternative bands. These are 5ghz bands that are available but the government requests the right to ask you to stop using them in an emergency
- So in a heavily congested 5ghz network this can be a lifesaver. This option should be added to DD-WRT sometime.

So is it worth it?

For me the answer is yes. It enabled me to get around a problem with my parent's TV pretty easily by reusing old hardware.

I'm disappointed the Nighthawk isn't working well with DD-WRT yet. I try it out every now and then but am still having issues. I also haven't turned in a bug report so it is partially my fault.

For my isolated network the ability to do have it separate is very nice. May flip from DD-WRT to OpenWRT to get SCAPY on it.

So is it worth it? (cont'd)

Am considering putting together OpenWRT and Tor to create a custom SSID on my network that will put all traffic over the Tor network without additional configuration. Will probably use the 841n we flashed tonight as part of it.

GPL Note

A lot of the GPL actions that have been taken have been based on manufacturers using GPL code for the networking software in their routers. Germany has done this a bunch with settlements every time.

When the GPL is finally tested in court there is a good chance it will be because of a router issue.

By GPL here I don't just mean the Linux Kernel, but BusyBox and other utilities used by the routers.

FCC Issue

TP-Link one of the most popular router manufacturers for alternative firmware announced they would no lock their devices and not permit different firmwares on them. They did this because they believed it was an FCC requirement. The FCC clarified this wasn't the case and TP-Link reconsidered.

Keep in mind this could change in the future. The FCC might get involved down the road. One of the things you can do with an alternative firmware is change the bands you're using to those of another country and that could be an FCC violation.

Life Hacker

Life Hacker has a lot of good articles about things you can do with DD-WRT/OpenWRT to improve quality of life.

Worthwhile to head out to their webpage http://www.lifehacker.com and do a search for dd-wrt and openwrt.

Easiest/Cheapest way to get Started

If you don't have an old router that will work with an alternative firmware. Head down to the Goodwill on 72nd & F and look for a router that is in the DD-WRT database on your phone.

Or consider buying off Amazon. Keep in mind you might get a different version of the router that might not be supported so being able to see the actual router before hand is a plus.

Q & A

Thanks.

Links

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

OpenWRT: http://www.openwrt.org

Tomato: http://www.polarcloud.com/tomato