Contents

Overview

The WRT610N was a top-of-the-line consumer Linksys device (replaced by the E3000) with the following features:

- Dual-radio (two BCM4322) allows to operate 2.4 Ghz B/G/N and 5 Ghz A/N simultaneously
- 4+1 port Gigabit switch (BCM53115)
- v1 300 MHz (BCM4705) / v2 533MHz (BCM4718) or 480MHz (BCM4716)
- USB 2.0 host port
- 64 MByte RAM, 8 MByte Flash

CFE Versions

The CFE is the bootloader (like a PC BIOS/UEFI) for Broadcom devices. It's responsible for initial hardware configuration and subsequent booting of the (Linux OS) firmware. There are several variants of the WRT610N CFE. To find the CFE versions from within DD-WRT, run this from telnet/ssh, or use the Web GUI via "Administration->Commands->Run Commands":

```
root@ap-ssn:~# nvram show|egrep 'bootnv|pmon'
bootnv_ver=6
pmon_ver=CFE 4.175.64.12
```

The versions are:

- bootnv_ver=6, pmon_ver=CFE 4.175.64.12 (subsequently called CFE .12)
- bootnv_ver=7, pmon_ver=CFE 4.175.64.16 (subsequently called CFE .16)
- bootnv_ver=18, pmon_ver=CFE 5.10.56.51

Builds between 12387 and 12424 do not work on CFE .12 models. See <u>ticket 1149</u>

- DD-WRT will start, but immediately reboot, requiring debricking.
- This is fixed in EKO build 12427, available <u>here</u>.
- *NOTE:* Eko builds have disappeared - use recommended build 14929 as a minimum.

Initial Flash Information

If installing DD-WRT for the first time on your WRT610N, you need to use a trailed (hardware-specific) build:

- **Initial flash for v1 only:** <u>(14929) dd-wrt.v24_mega_wrt610n.bin</u>
- **Initial flash for v2 only:** <u>dd-wrt.v24-14929_NEWD-2_K2.6_mini_wrt610nv2.bin</u>
- **Alternately use** *<u>https://download1.dd-wrt.com/dd-wrtv2/downloads/</u>* in place of *<u>ftp://ftp.dd-wrt.com/</u>*

Then upgrade to a newer good generic build (non-trailed build like mega.bin). For more build information see <u>here</u>.

Linux Kernel Builds

- DO NOT USE K3X on V1, NOR K24 on V2, OR YOU MAY BRICK YOUR ROUTER!

For (most) Broadcom MIPS routers, DD-WRT has three branches: *broadcom* using the 2.4 kernel, *broadcom_K26* (2.6 kernel), and *broadcom_K3X* (3.10 kernel). You can install the K2.4 builds on v1, but not v2. K2.6 supports both v1 and v2. To identify the difference, K2.4 builds aren't usually marked with any special identification, but K2.6 builds are in "broadcom_K26" folder with "K2.6" in the filename. K3.X is similar but supports v2 only.

For example, these are 2.4 kernel builds, only for v1 routers (**THESE ARE NOT FOR INITIAL FLASH**):

- <u>(14929) dd-wrt.v24_mega_generic.bin</u>
- <u>(14929) dd-wrt.v24_usb_generic.bin</u>

These are 2.6 kernel builds and will work on v2 as well as v1:

- <u>dd-wrt.v24-14929_NEWD-2_K2.6_big.bin</u>
- <u>dd-wrt.v24-14929_NEWD-2_K2.6_std_usb_ftp.bin</u>

Note: not all builds support USB. See <u>Build Types</u>

- K3X did not yet exist in 14929, see below or research New Build and model-specific forum threads.

Latest version

Update here: <u>latest downloads</u> Use the WRT610Nv2 mega file in the K26 or K3X folders. **Make sure the build is less than 8 000 000 bytes before flashing it.**

note from tmittelstaedt - this is still broken in build 33555 Mega <u>[1]</u>

The WRT610N has two radio modules and thus two wireless devices with distinct configuration in DD-WRT:

- *wl0* is the 2.4 Ghz band radio (supporting 802.11b/g/n)
- *wl1* is the 5 Ghz band radio (supporting 802.11a/n)

Note that Draft-N can operate in both the 2.4 and 5 Ghz bands.

Steps for flashing

1. <u>Hard reset</u>
2. Navigate to the firmware update tab in the Linksys or dd-wrt GUI
3. Initial flash: use the trailed build (610n in the filename), otherwise not required
4. Wait 5 minutes after flashing
5. Power cycle the router
6. <u>Hard reset</u> again
7. Configure the router

Reversion to OEM Firmware

To revert to the original firmware, just download and flash the <u>Linksys firmware</u> using the DD-WRT GUI, following the same steps outlined in the "Steps for flashing" section above.

Recovery (Unbricking)

A simple way to recover a bricked device (confirmed to work with both CFE.12 and CFE.16) is:

1. unplug all ethernet ports **(Important!)**
2. unplug power
3. plug power in
4. wait 2-2.5 seconds
5. press the reset button and *keep it pressed* for 5 seconds, then *release it*
6. reconnect ethernet (DHCP shoud give IP address to computer)
7. point your browser at 192.168.1.1. You should see a "Management Firmware update" screen where you can flash the original firmware or dd-wrt directly (even mega builds).

Alternative Method 1:

1. manually assign 192.168.1.10 to your computer
2. unplug power

   3. plug power in
   4. wait 0.5-1.0 seconds
   5. press the reset button and *keep it pressed* for 1 second, then *release it*
   6. point your browser at 192.168.1.1.

Alternative Method 2:

1. manually assign 192.168.1.10 to your computer
2. unplug power
3. plug power in
4. wait for all lights blink
5. press the reset button and *keep it pressed* for 1 second or 3/4 flashes of the power-light, then *release it*
6. point your browser at 192.168.1.1.

The alternative methods are reported to work well on the wrt-610Nv1 CTGxxxx series (mostly works at the first attempt); these series are using CFE .16

On occasion, the recovery method will not accept a new dd-wrt image. Download the latest official WRT610N firmware from linksys and flash it back to the router via recovery method. Once the router is back online and you can navigate to the web gui, reflash dd-wrt to the router.

The management mode can also be activated from the serial console using

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

Known Issues

Unstable WLAN (especially when wl1 radio is enabled)

It seems that the WRT610n rev 1 and 2 have some issues when the wl1 (5ghz) interface is enabled, which have been experienced from r13064 to r14929 so far. When wl1 is enabled and WPA is activated, the router randomly disconnects its clients.

The apparent solution is to avoid any use of TKIP on the wl1 radio, and stick to AES encryption only (this does not work for everyone).

10 MBit fails (causing WoL issues)

The on-chip switch currently doesn't properly support transitions from 100 Mbit/Gigabit to 10 Mbit; it will not renegotiate/fallback but stay in the previous mode, rendering the connection unusable. This is often a problem when Wake-On-Lan is to be used and the station to be woken switches to 10 MBit in standby mode for power preservation. Workaround for this case: some network interfaces allow setting the speed to be used for WoL idle mode, set this to 100 MBit.

Random reboots/WLAN lockups (FIXED since 13xxx)

As of build 12427, the router will randomly reboot, sometimes after minutes, sometimes after hours. Using only the 2.4 Ghz radio seems to make the problem occur less often. Developers are aware of the problem and are working on it.

A possible workaround seems to be disabling the interference mitigation mode using

```
wl -i eth0 interference 0
wl -i eth1 interference 0
```

either from telnet or from Administration->Commands.

See here (signature) for real world uptimes of 3 different WRT610N devices, including their respective configurations.

Fixed Wireless MAC (FIXED SINCE 12360)

Until build 12360, the 2.4 Ghz wireless radio MAC is always 00:90:4C:4E:00:2A. This causes weird client behavior if you have more than one WRT610N in one network. As a workaround, you can manually set the mac address using the shell commands

```
nvram set "pci/1/1/macaddr"=00:90:4C:D6:02:2a
nvram commit
```

This is fixed in 12427 for CFE.16 devices. For CFE.12 devices, the situation is now reversed: The 5 Ghz MAC always has 00:90:4C:4E:00:2A, and the 2.4 Ghz MAC is fine.

VLAN Support

See VLAN Support.

5 Ghz specific issues

- For certain builds the 5 Ghz radio (wl1) may only work when the wireless mode is set to *NA-Mixed*. Later builds e.g. 13972-mega [2] do not exhibit this behaviour.

- Neither Site Survey nor Wizviz Survey currently work for the 5 Ghz band.

No TFTP recovery

(not really an issue anymore) Due to a problem in the CFE, it is not possible to recover a bricked device using the commonly recommended boot-wait TFTP process (i.e. by waiting for the device to react to pings to 192.168.1.1 and TFTP a firmware file to it). TFTP transfers to the device which are larger than 3.8MB (i.e., the stock firmware) will fail, other TFTP transfers will seemingly succeed, but the CFE will not flash them. See above for a much simpler way to unbrick using management mode. Debricking via serial port is also

possible. Note that the serial port is externally accessible inside the "Internet" ethernet jack. Instructions for serial recovery are available here: http://www.dd-wrt.com/phpBB2/viewtopic.php?p=209668#209668

PPPoE does not work with builds above 15506

The most current SVNs introduce an issue where the router becomes unresponsive as soon as PPPoE is activated for the WAN port. An ongoing discussion can be found here: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=88260

Other notes

USB

USB support works, including Hubs, for all kind of devices, even when Linksys only advertises this as a "Storage Link". Note that there are known Linux USB issues with USB 2.0, Hubs and Full/Low speed devices, notably the often used FTDI serial converters. Use USB 1.1 only as a workaround.

5 Ghz channels

Not specific to the WRT610N, but with the 5 Ghz band, the channel limitations per regulatory domain are much broader than with 2.4 Ghz channels. Since dd-wrt doesn't limit the 5 Ghz channel selection, you run a much higher chance of setting the router to a channel which your client device (which does honor regulatory limits) doesn't support. See http://en.wikipedia.orghttp://forum.dd-wrt.com/wiki/List_of_WLAN_channels#5.C2.A0Ghz_.28802.11a.2Fh.2Fj.2Fdr for a list of available 5 Ghz band channels.