

# NETGEAR WNR3500L Open Source Wireless N (Draft) Router Open Source Guide & Resources

## *Chipsets:*

CPU: Broadcom BCM4718 (Draft IEEE 802.11n compliant)

- Four way set associative 32-KB instruction cache
- Two way set associative 32-KB data cache
- 64 entry translation look aside buffer (TLB)
- Dual band radio transceiver
- Two integrated USB 2.0 EHCI host ports
- A 8/16-bit parallel external bus interface (EBI)
- Enhanced 10/100/1000 Ethernet MAC controller with TCP segmentation and checksum upload

Switch : Broadcom BCM53115s

- It enables deployment of GIGABIT ethernet.
- It contains non-blocking 5-port 10/100/1000 switch silicon that integrates
- Five 10/100/1000 PHYs.
- Two fully integrated GMII/RGMII/MII interfaces , two IMPs (Inband management ports)
- It provides four selectable QoS per port .

## *Memory*

- SDRAM: 32 MB
- Flash : 8 MB

## *Memory used by the latest router firmware:*

SDRAM :

- Flash : 5.2 MB

## *Module and Software Specification*

- WNR3500L is running Linux 2.4.20.

The following table lists the functional modules of the WNR3500L router and the source and versions of the different modules. More information on these functional modules can be obtained directly from the source of the packages.

Module	Package	Version	Location
DHCP Client	Copyright (C) 1999	0.9.8	src/router/udhcpd/

	Matthew Ramsay < <a href="mailto:matthewr@moreton.com.au">matthewr@moreton.com.au</a> >, Chris Trew < <a href="mailto:ctrew@moreton.com.au">ctrew@moreton.com.au</a> >		
DHCP server	Copyright (C) 1999 Matthew Ramsay < <a href="mailto:matthewr@moreton.com.au">matthewr@moreton.com.au</a> >, Chris Trew < <a href="mailto:ctrew@moreton.com.au">ctrew@moreton.com.au</a> >	0.9.8	src/router/udhcpd/
DNS Proxy	Copyright (c) 2000 Simon Kelley	1.10	src/router/dnsmasq/
VLAN	Copyright (C) 2001 Ben Greear	1.6	src/router/vlan
Wireless Driver	Broadcom	Precompiled	src/wl/linux
UPnP	Copyright (C) 2008, Broadcom Corporation	Precompiled	src/router/bcmupnp/upnp
Bridge	Copyright (C) 2000 Lennert Buytenhek	1.1.1.1	src/router/bridge/
Busybox	Copyright (C) 1999,2000,2001 Erik Andersen	0.60.0	src/router/busybox/
DHCPv6 client/server	Copyright (C) 1998 and 1999 WIDE Project.	1.1.1.1	src/router/dhcp6/
Web server	Copyright © 1999,2000 by Jef Poskanzer	Precompiled	src/router/httpd/
IGMP	Copyright (C) 2008, Broadcom Corporation	Precompiled	src/router/igmp/prebuilt
IPTABLES	Copyright (C) 2000-2002 by the netfilter coreteam , Paul 'Rusty' Russell ,Marc Boucher, James Morris, Harald Welte , Jozsef Kadlecsek	1.2.7a	src/router/iptables/
NTP client	Copyright 1997, 1999, 2000 Larry Doolittle		src/router/ntpclient/
PPP	Copyright (c) 1989 The Carnegie Mellon University	2.3.11	src/router/ppp/
Router Advertisement daemon(radvd)	Copyright 1996-2000 Pedro Roque, Lars Fenneberg	0.9.1	src/router/radvd/

User init	Copyright (C) 1995, 1996 by Bruce Perens		src/router/busybox/init.c
ifconfig utility	Bjorn Wesen, Axis Communications AB	1.2	src/router/busybox/ifconfig.c
Ethernet Driver	Broadcom	precompiled	src/et/linux/

## Making a Console Debug Interface for WNR3500L

### *Source Code and Executable:*

This section describes the steps to download the source code and toolchain, install the toolchain, compile and link the existing source code, and add user applications. FC6 was used for development throughout this guide.

1. Download the complete archive from NETGEAR web site.
2. Unpack the source code.
3. Install the tool chain using following steps :
  - cd /opt
  - mkdir brcm
  - cp hnd-tools-3.2.3.tgz to /opt/brcm
  - tar -zxvf hnd-tools-3.2.3.tgz
  - export PATH = /opt/brcm/hndtools-mipsel-uclibc-3.2.3/bin : \$PATH and
  - export PATH = /opt/brcm/hndtools-mipsel-linux-3.2.3/bin : \$PATH
- 4 . Compile the source code:
  - Go to src/router folder of your source distribution.
  - Give make menuconfig to select router packages and linux components that should be compiled.
  - Save the customized router package and linux kernel configuration and exit.
  - Run make dep.
  - From src/ directory give “make” to compile the code . This will create a .trx file in the image/ directory which should be flashed to WNR3500U.

## Custom Applications on Open Source Router:

To develop any custom applications on this router, please follow the following steps.

Adding new applications :

- Copy application XXX in the directory src/router.

- Rename the application directory to xxx.
- Add the new application to the file src/router/config/Config

config CONFIG\_XXX

bool "XXX Application"

depends on YYY (If depends on YYY otherwise skip the line)

help "This is the New Application"

Answer Y for application XXX.

- Add the new application in the file src/router/Makefile

...

obj-\$(CONFIG\_XXX) += xxx

...

- Write a make file in xxx directory as required for the application. Also keep in mind that the executable name must be xxx.

[[page]]

## Setting up a Serial Port Connection to Access the WNR3500L Board:

If you're going to be working with your router a lot, or especially working with multiple routers, it's convenient to have an externally accessible serial port. However, you should remember that soldering third-party circuits to your router's mainboard voids the warranty, and if you make a mistake, you can cause permanent damage to your router. Proceed at your own risk.

### *Items Needed:*

- An FTDI 3.3V USB-to TTL serial cable (TTL-232R-3V3)-1.8 m
- diagonal cutting pliers (optional).
- needlenose pliers (optional).

### *Installation:*

WNR3500L comes with an inbuilt serial cable header. You just need to open your router box to see it.

It has been shown in the figure below:



The USB-Serial cable initially looks as follows:



As all pins on the serial end of the cable are not useful ( We need only three pins) we need to open the serial end of the cable and separate three pins that are useful to us from the rest of the pins.

These pins are :

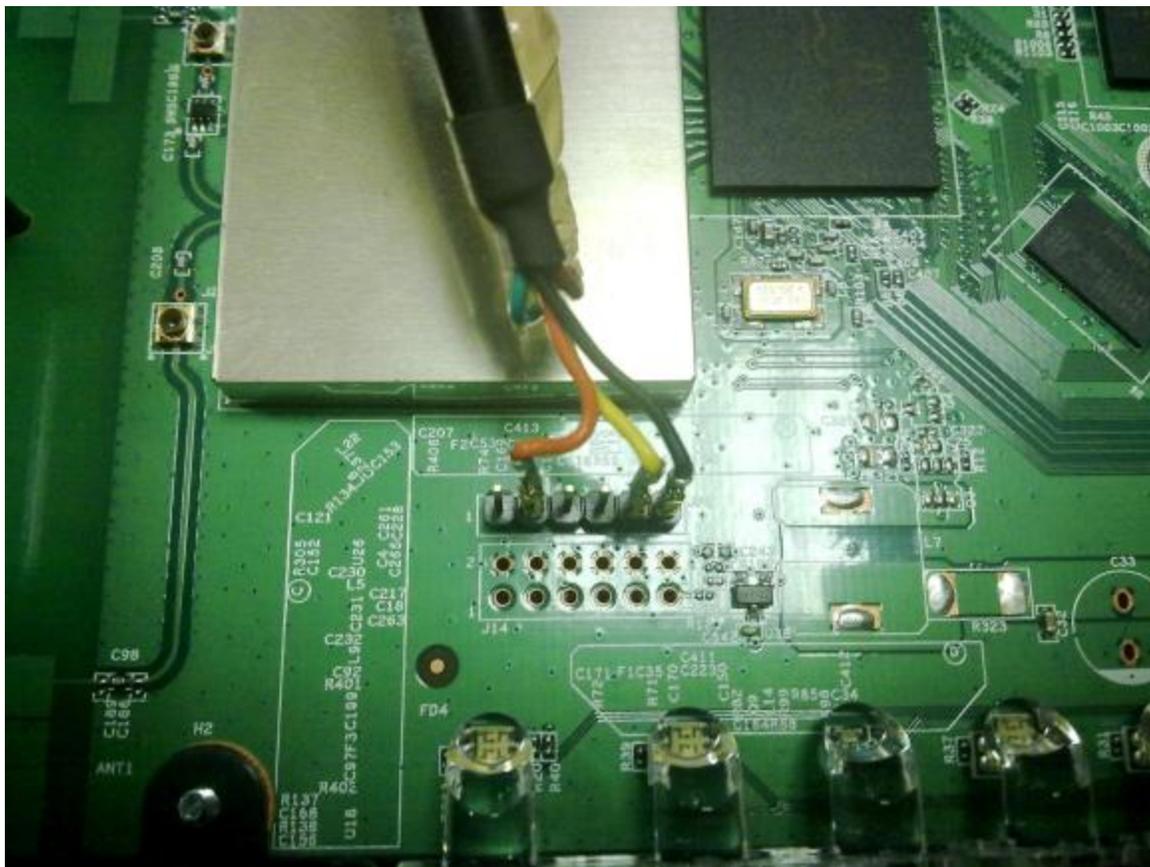
Pin 1 (GND pin): Black coloured , it is connected to pin 6 of serial header.

Pin 4 (Tx pin) : Orange coloured , it is connected to pin 2 of serial header.

Pin 5 (Rx Pin) : Yellow coloured , it is connected to pin 5 of serial header.

The figures given below show the USB-Serial cable after the above mentioned modification and how it is connected to the serial header of WNR3500L.





That's it - your setup is ready!

## WNR3500L Firmware Upgrade Using Serial Console

The firmware can be updated using one of two methods; you can either use the serial console or the GUI. First, we'll describe the method for the former, using the cable you just created. The steps to flash the router using serial interface are as follows:

(One can use minicom, PuTTY or other similar utility for this, I have used minicom.)

- Connect the serial end of the cable to the serial header of your board and USB end to your host PC. Make sure the putty/minicom windows is in front.
- Power on the board.
- As soon as you power on the board, you have to hit control-C to enter the CFE prompt. You may have to hit it a couple of times.

If you are successful you will see this message :

```
CFE for WNR3500L version: v1.0.36
Build Date: Tue Aug 11 15:09:14 CST 2009
```

```

Init Arena
Init Devs.
Boot partition size = 262144(0x40000)
Found a 8MB ST compatible serial flash
et0: Broadcom BCM47XX 10/100/1000 Mbps Ethernet Controller 5.10.56.28
CPU type 0x19740: 453MHz
Tot mem: 65536 KBytes

Device eth0: hwaddr 00-24-B2-89-28-3A, ipaddr 192.168.1.1, mask 255.255.255.0
gateway not set, nameserver not set
Startup canceled
CFE> ^C
CFE> ^C
CFE> ^C

```

- At the CFE prompt type in tftpd. This will start a tftp server and you will get the following lines at the CFE prompt:

```

CFE> tftpd
Start TFTP server
Reading ::

```

- At your host PC make sure that you have an IP 192.168.1.x and this interface should be connected to one of the LAN ports of your board. Now go to the directory where you have kept the .chk file to be flashed and give the following command :

```
$ tftp -m binary 192.168.1.1 -c put firmware.chk
```

Once you give this command firmware upgrade will start. In PuTTY/minicom you should see something like this :

```

Reading :: Done. 5443642 bytes read
Programming...done. 5443642 bytes written
Write len/chksum offset @ 0x0074FFF8...done.
Decompressing.....done

```

```

CFE for WNR3500L version: v1.0.36
Build Date: Tue Aug 11 15:09:14 CST 2009
Init Arena
Init Devs.
Boot partition size = 262144(0x40000)
Found a 8MB ST compatible serial flash
et0: Broadcom BCM47XX 10/100/1000 Mbps Ethernet Controller 5.10.56.28
CPU type 0x19740: 453MHz
Tot mem: 65536 Kbytes

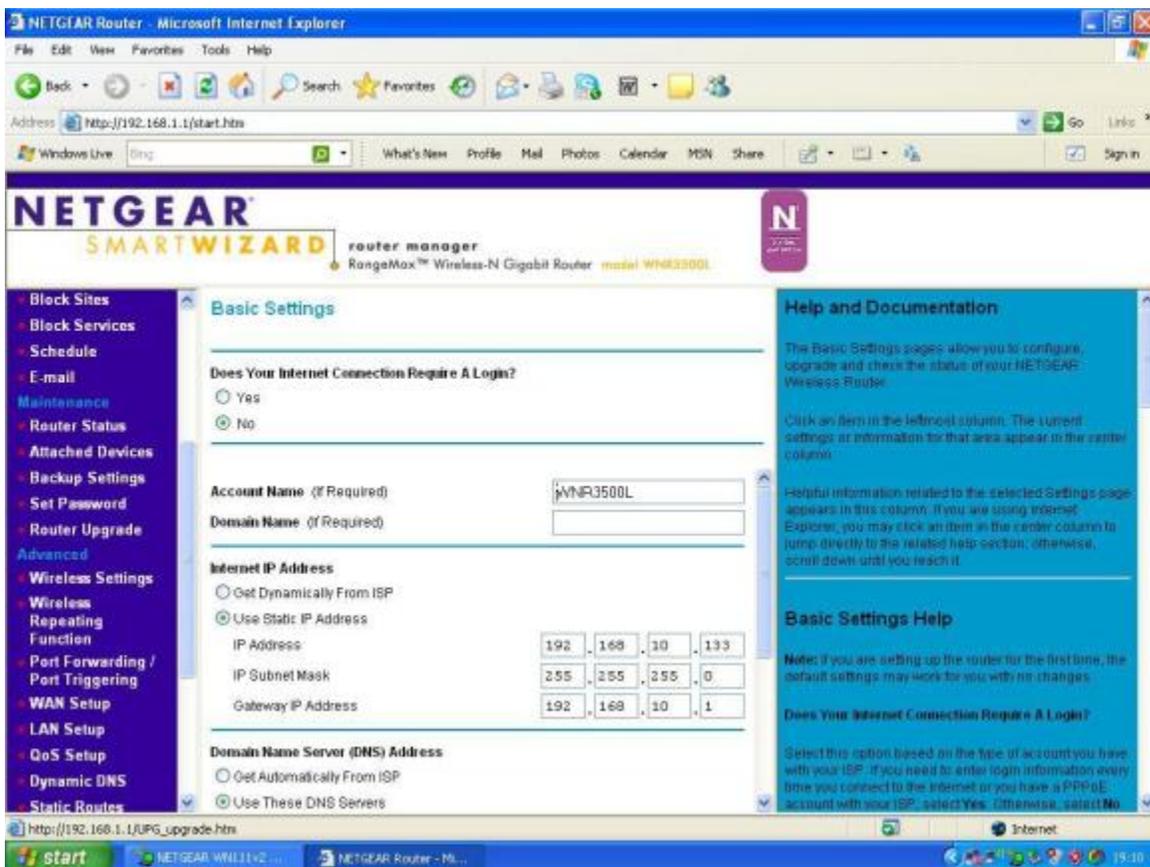
```

## WNR3500L Firmware Upgrade Using the GUI

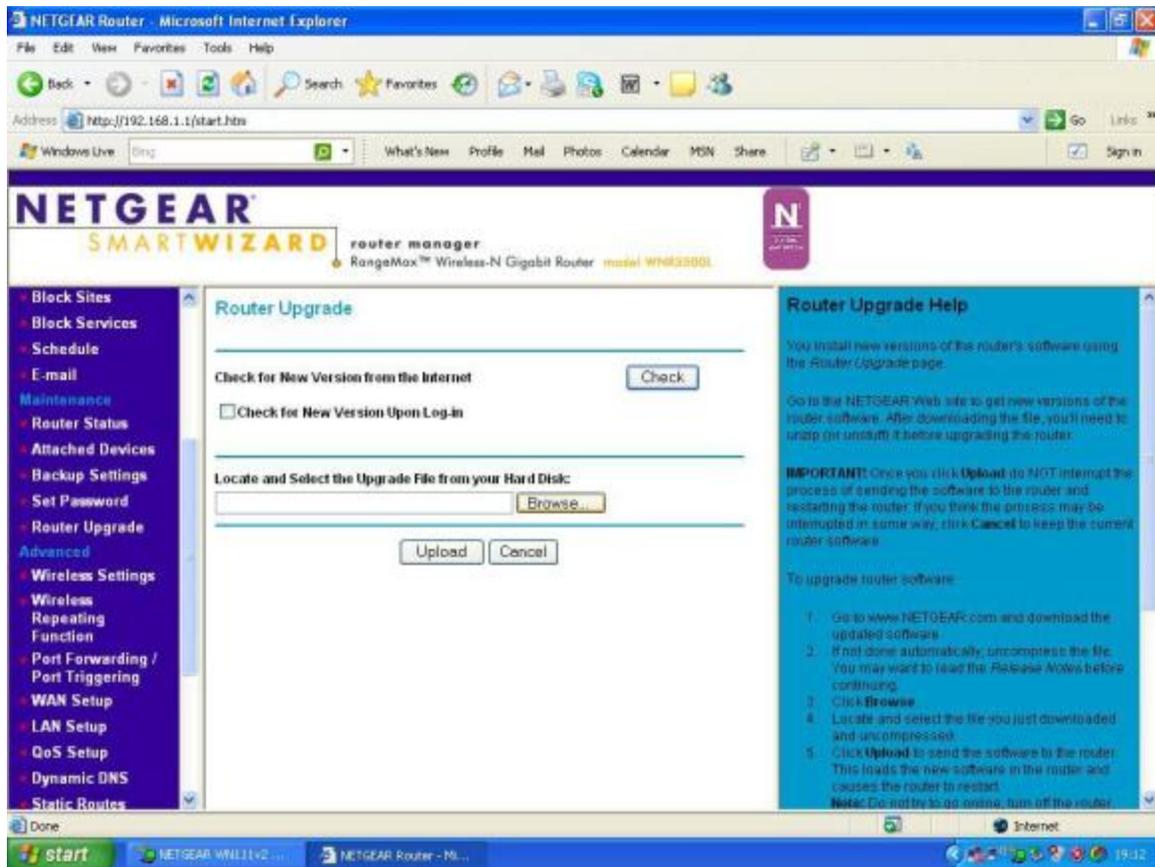
Firmware upgrade can be done by using the GUI of the firmware running on the board. We can upgrade third party firmwares from Default NETGEAR firmware and vice-versa.

*Performing upgrade from default firmware => Third party firmware:*

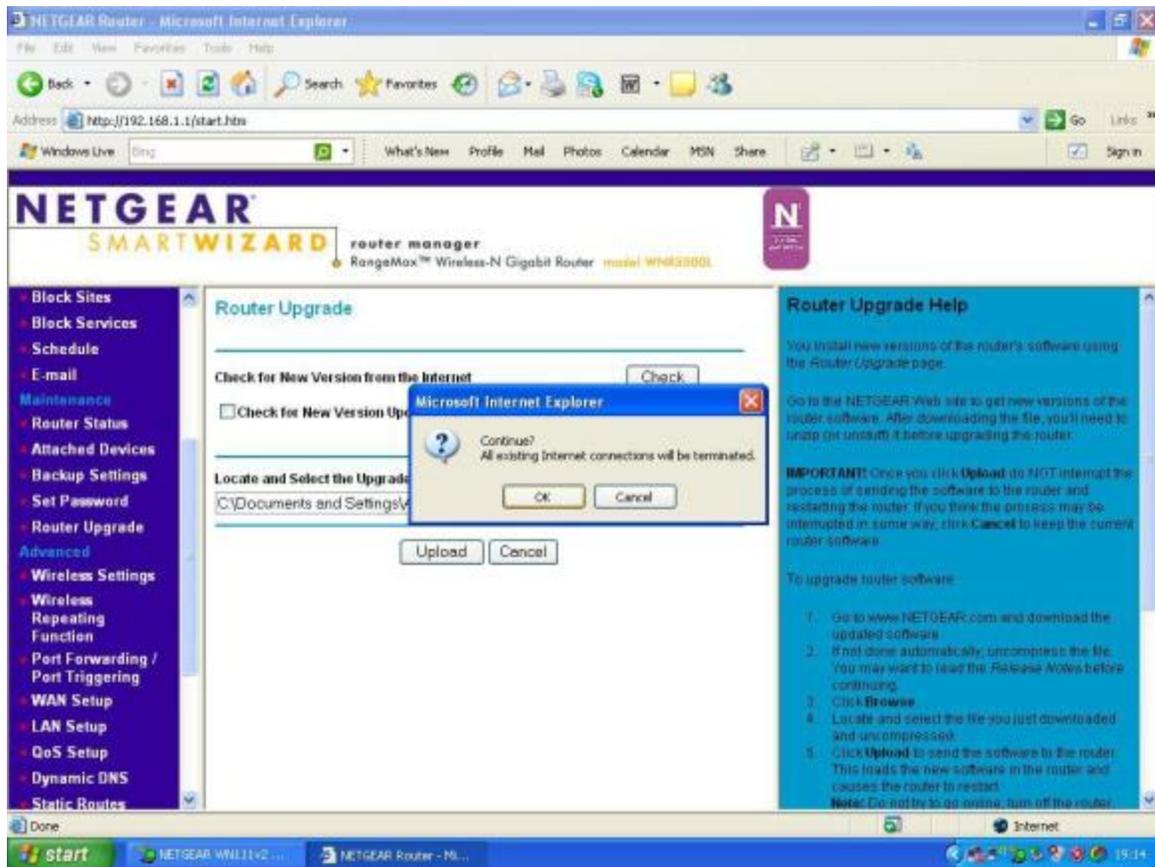
In NETGEAR GUI click “Router Upgrade”.



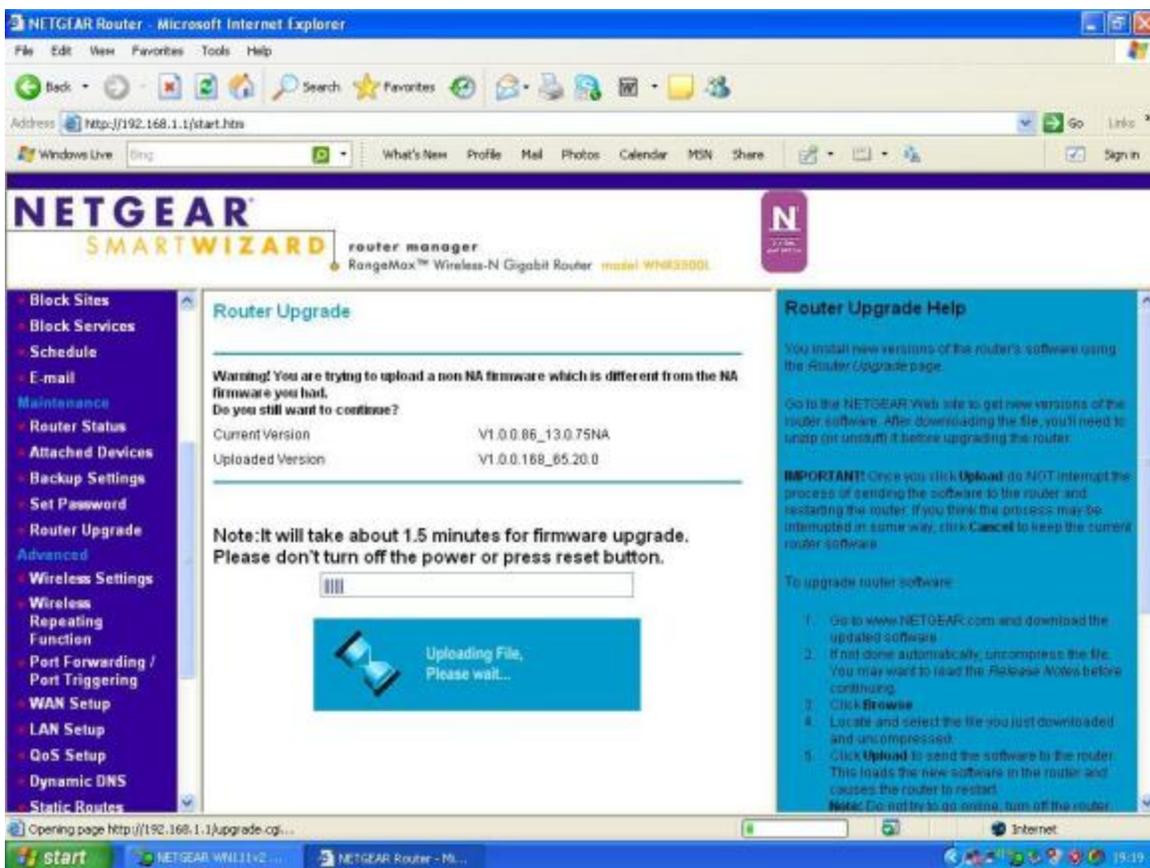
Clicking Router Upgrade shows the page shown below:



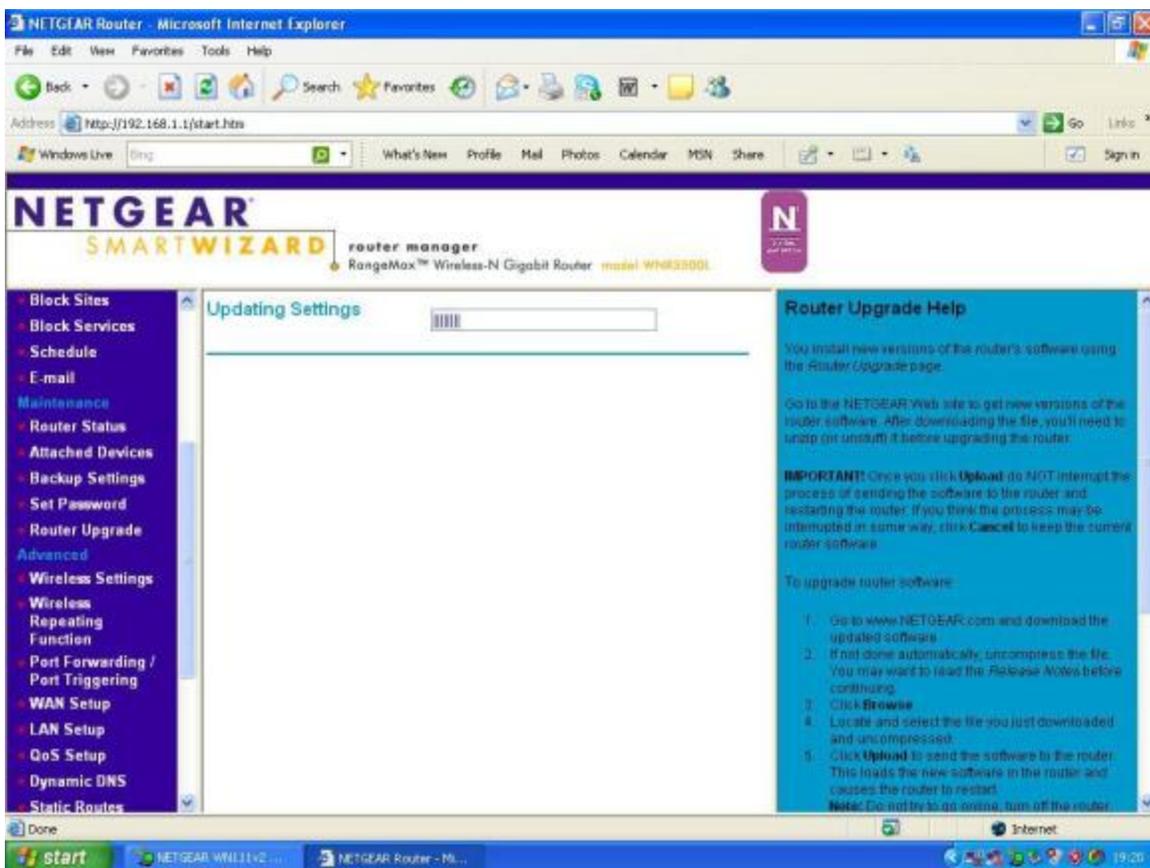
Click the browse button and select a file to flash. After selecting the file click upload. It will ask for a confirmation as shown below:



Click OK to continue. It also asks you if you want to upgrade to a non NA version. Once you reply, the upgrade starts as shown in the figure below:



It takes a few minutes to upgrade to finish and once the upgrade finishes you can see the confirmation page as shown below:

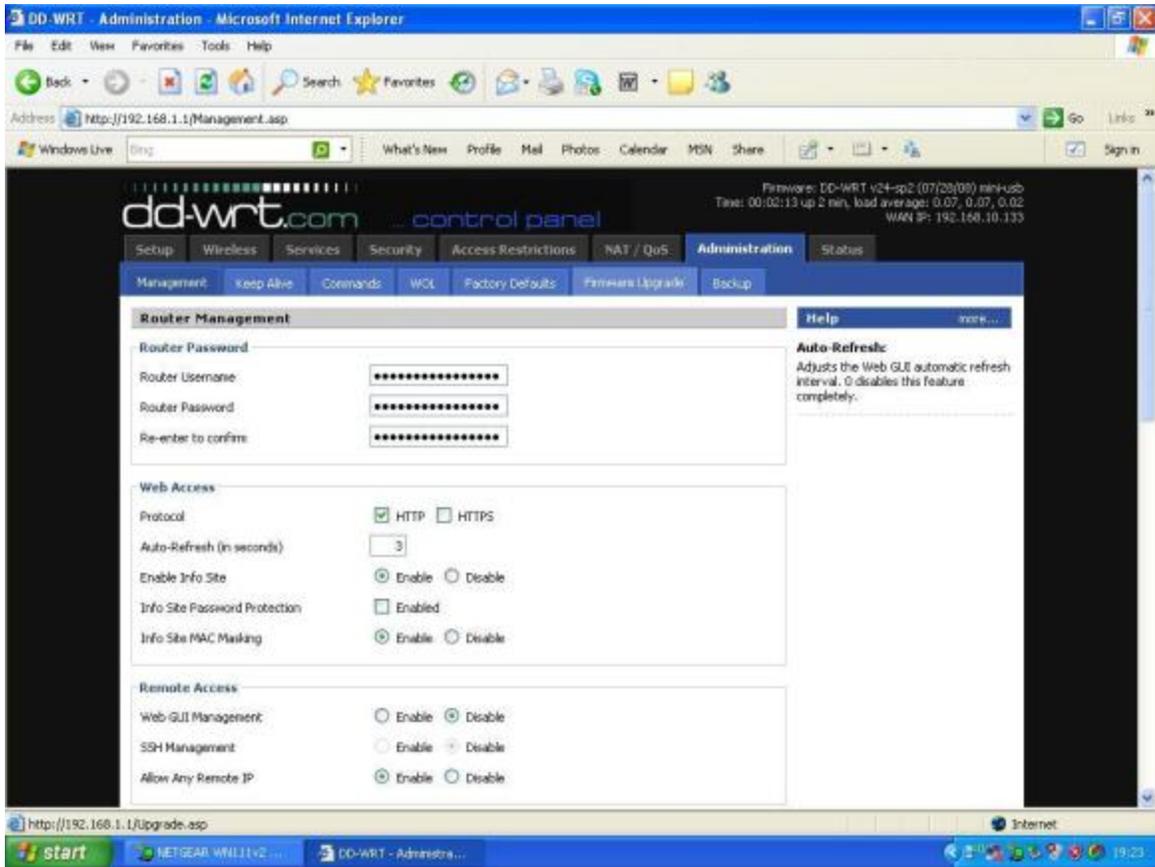


This indicates that upgrade is successful and the router is rebooting with the new firmware. After settings have been updated and flash process is over, one should do a hard factory reset to get proper nvram settings for the flashed firmware. This method can be used to flash any third party/Default NETGEAR firmware for WNR3500L.

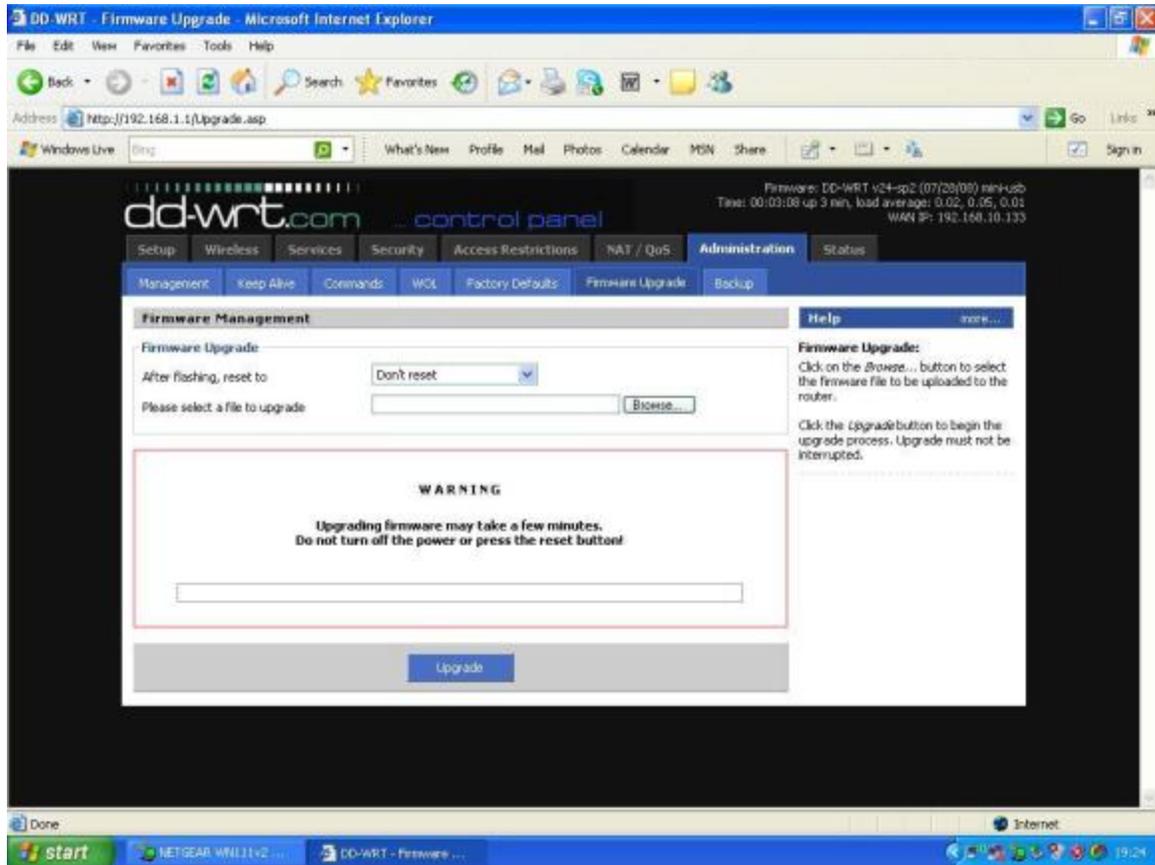
[[page]]

## WNR3500L Firmware Upgrade From DD-WRT

In the DD-WRT GUI click the tab Administration, it shows the following page :

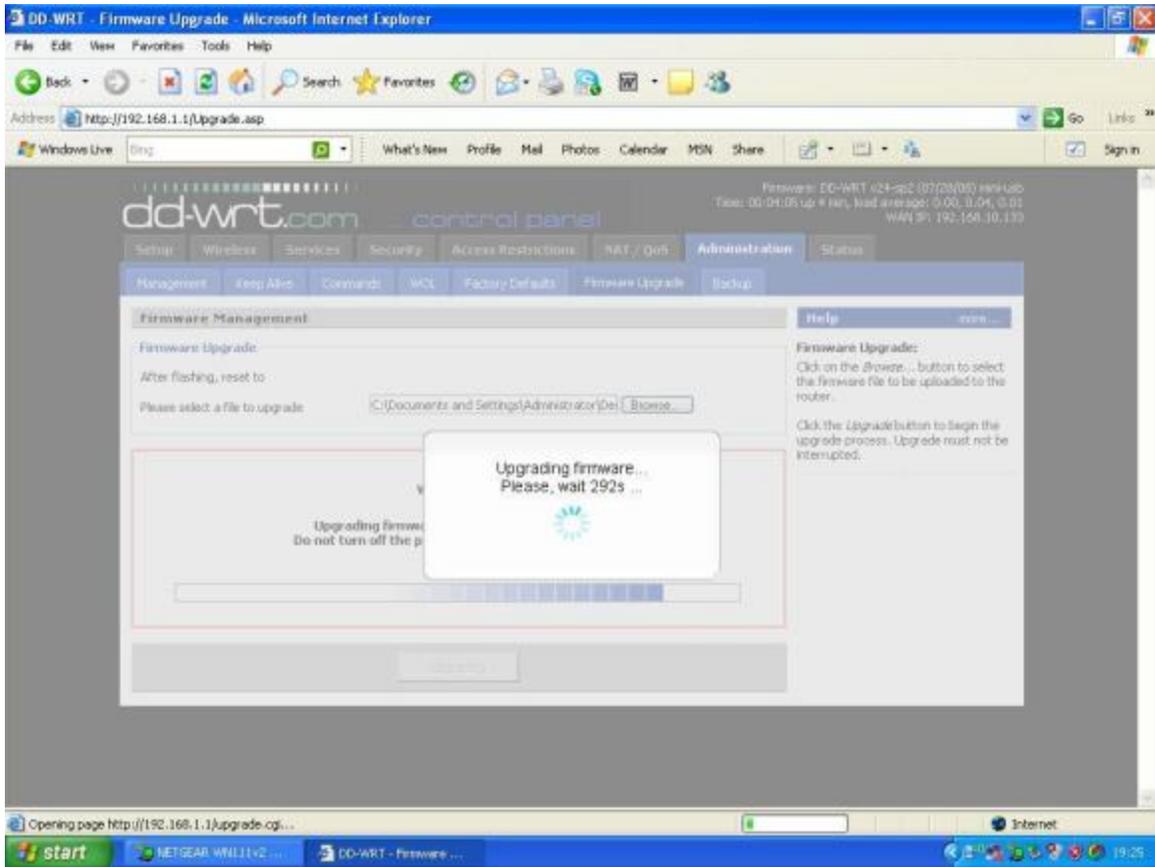


Now, click the tab Firmware Upgrade to go to firmware upgrade page:

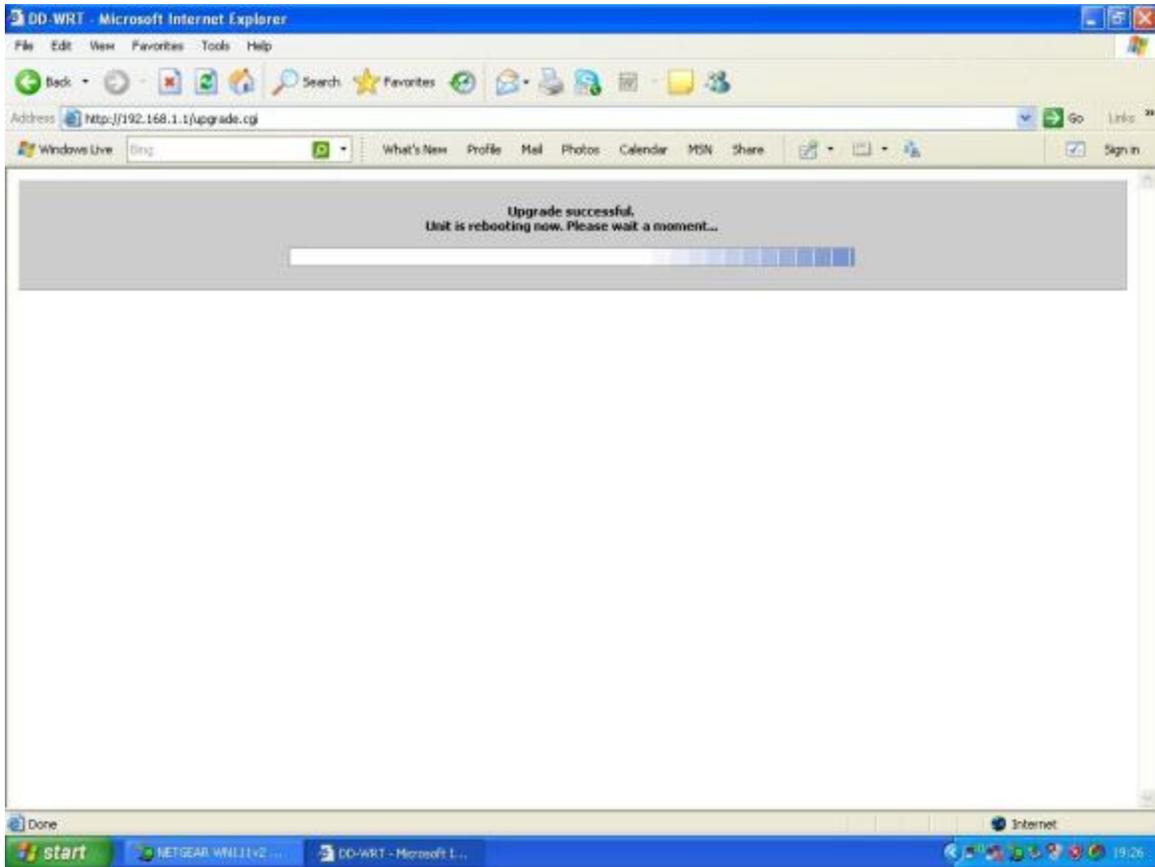


Click the browse button to select the file to flash and click upgrade.

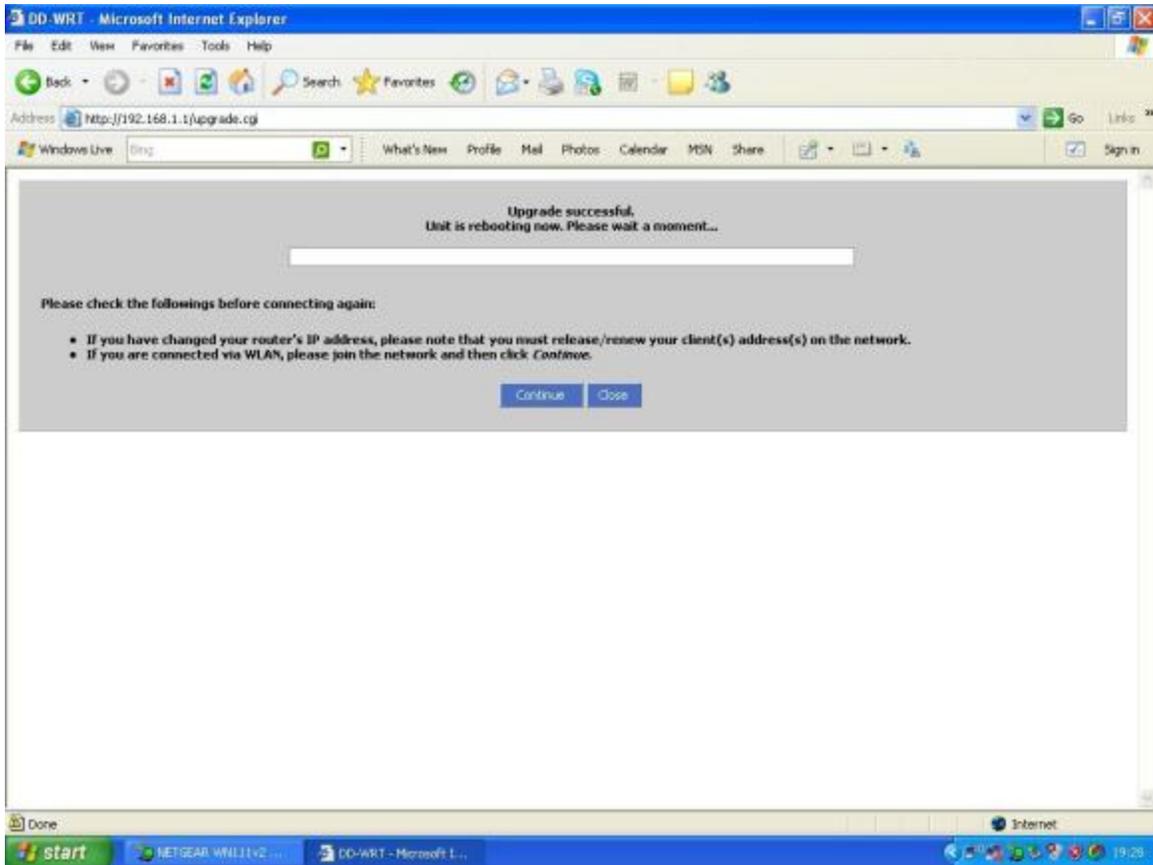
It will start upgrade process as shown below:



If the firmware upgrade is successful, you will see the following page.



Once the flash process finishes you will see the following page. Click continue to proceed.



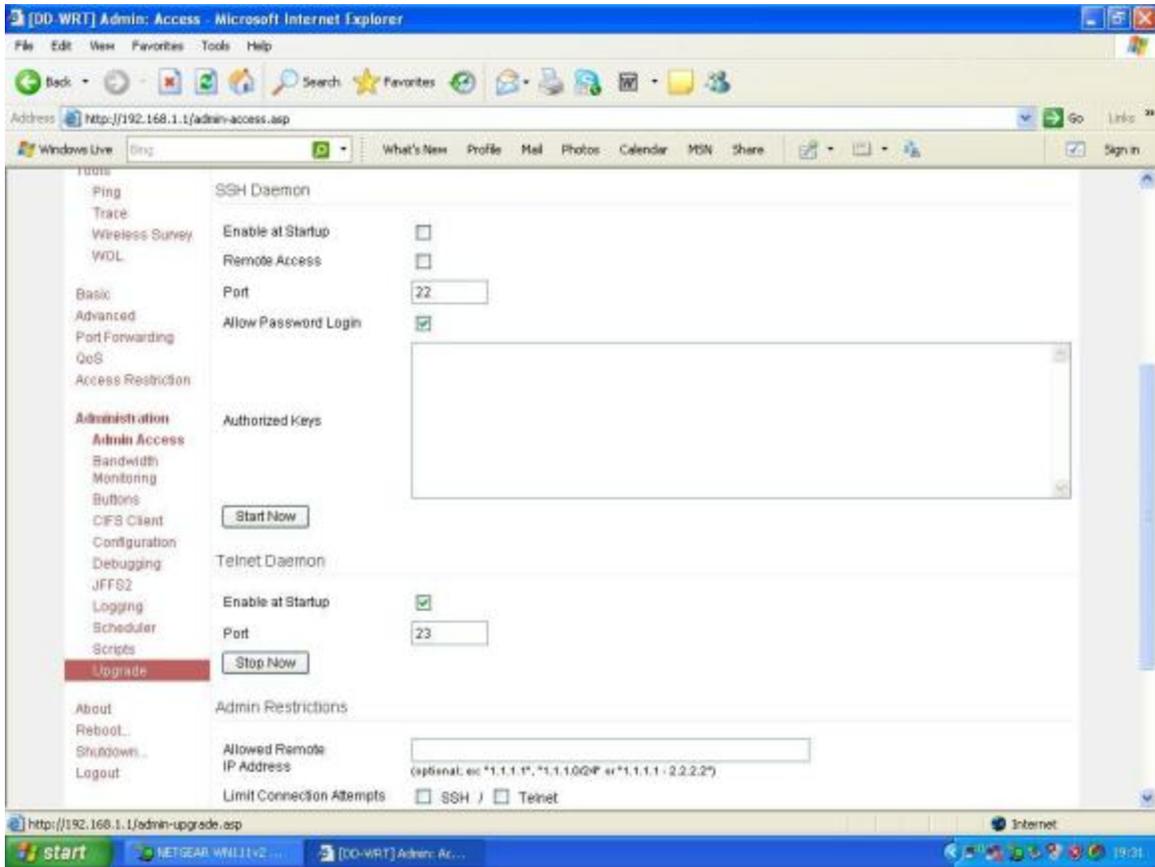
This is how a firmware can be flashed using DD-WRT GUI.

[[page]]

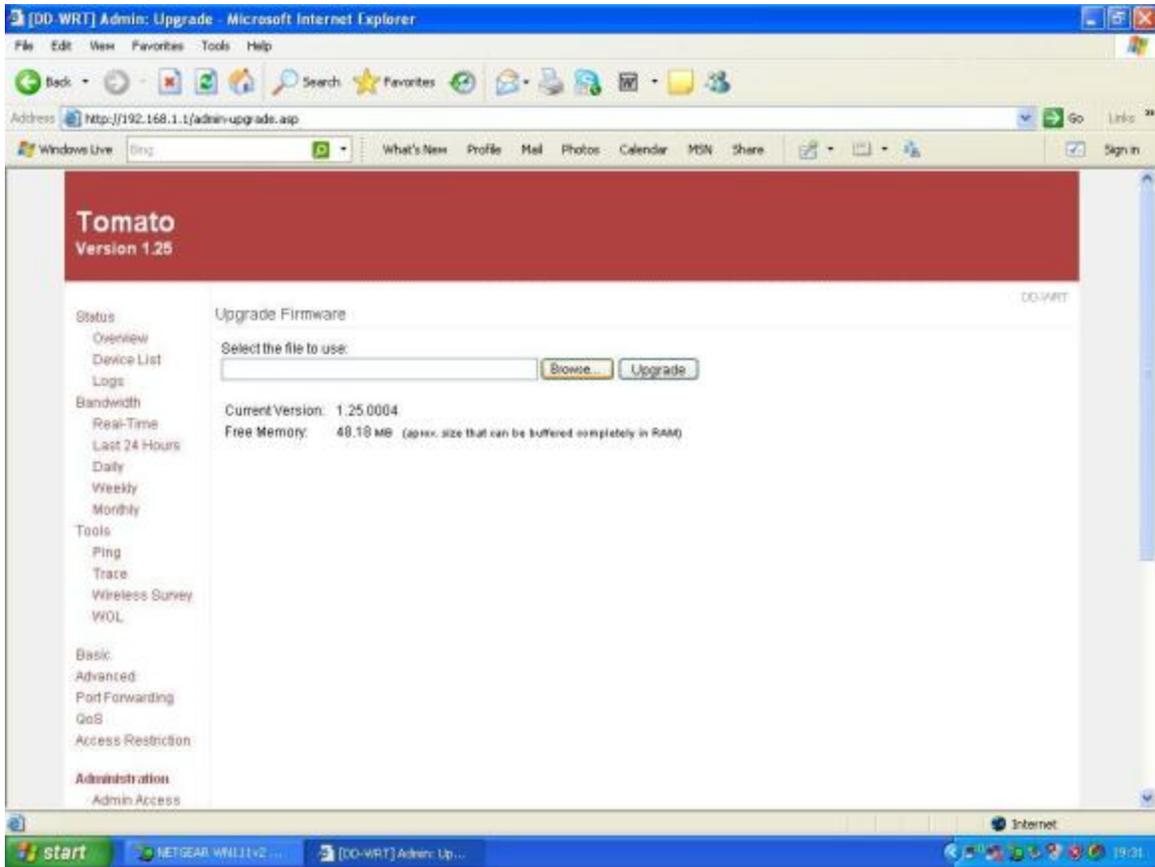
## WNR3500L Firmware Upgrade from Tomato:

To do firmware upgrade from Tomato GUI one needs to proceed as follows:

Click upgrade under Administration tab as shown in the figure below:

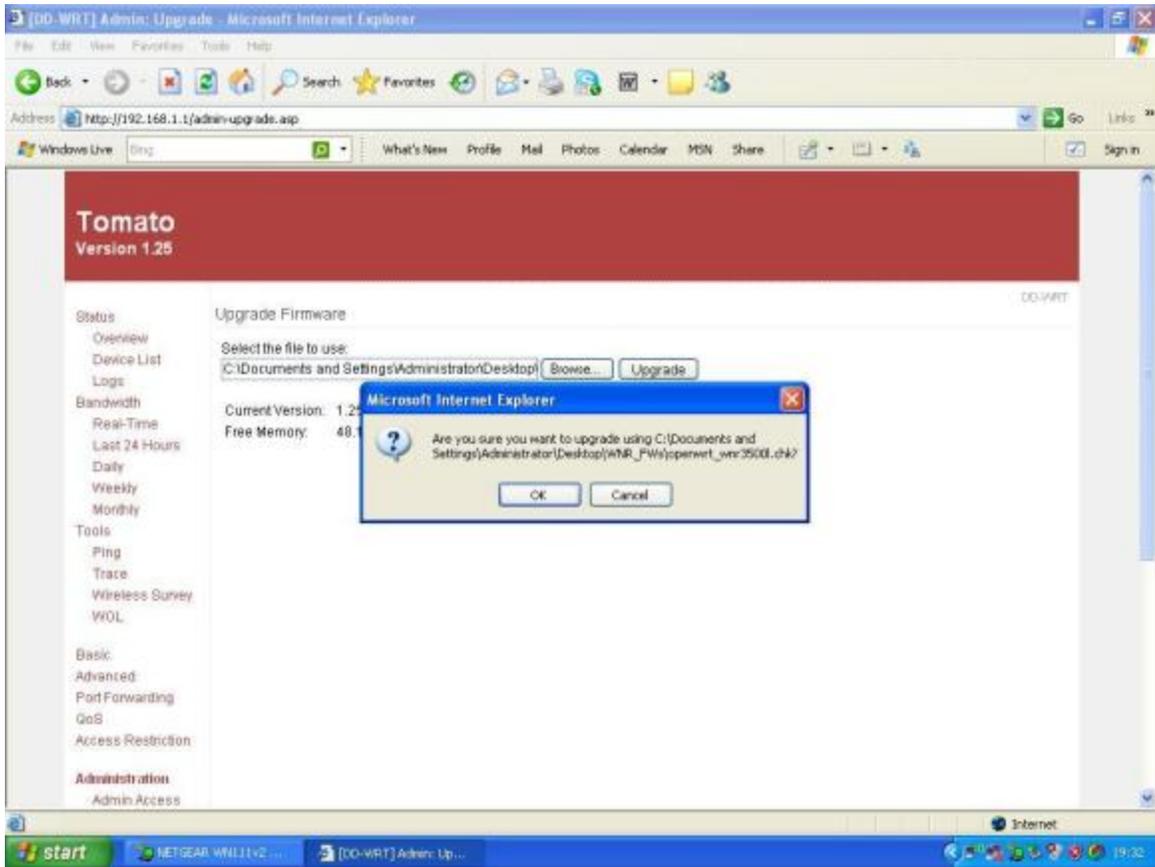


This will take you to firmware upgrade page which appears as the one shown below:

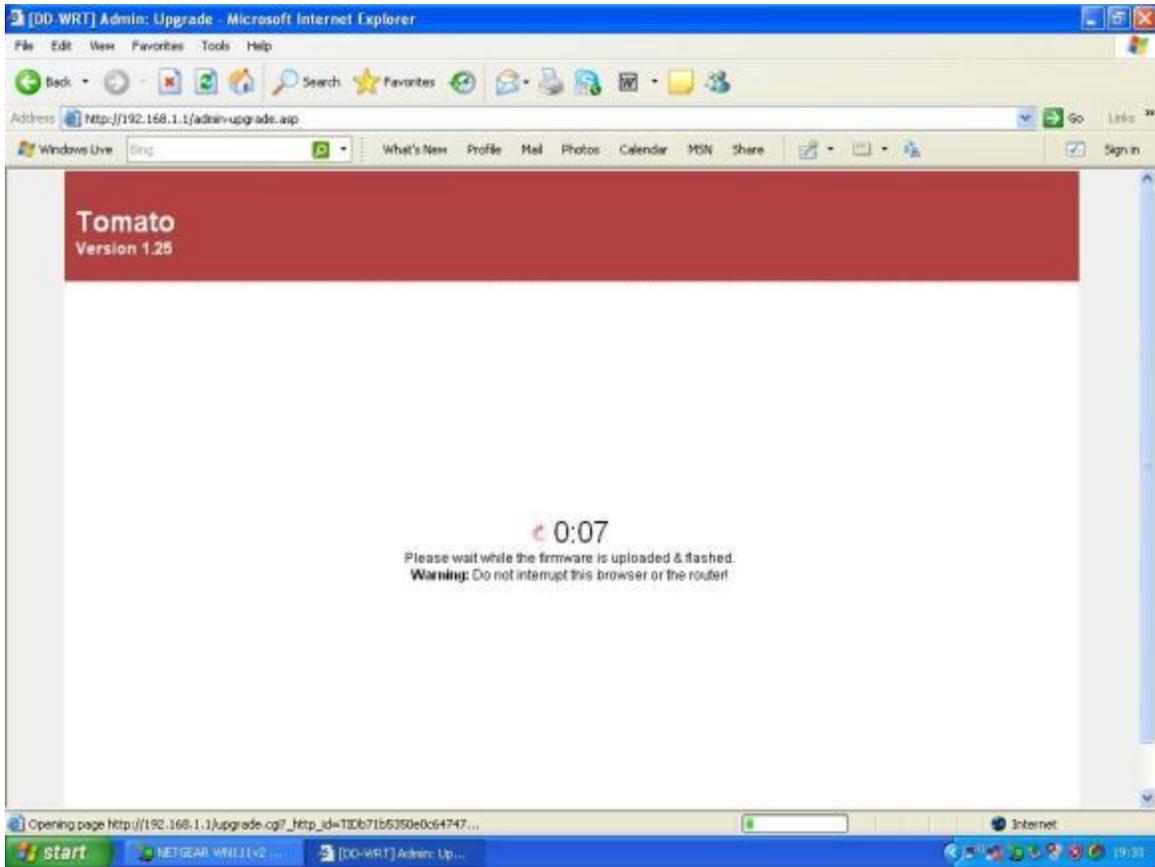


Click browse to select the file to upload and then click upgrade.

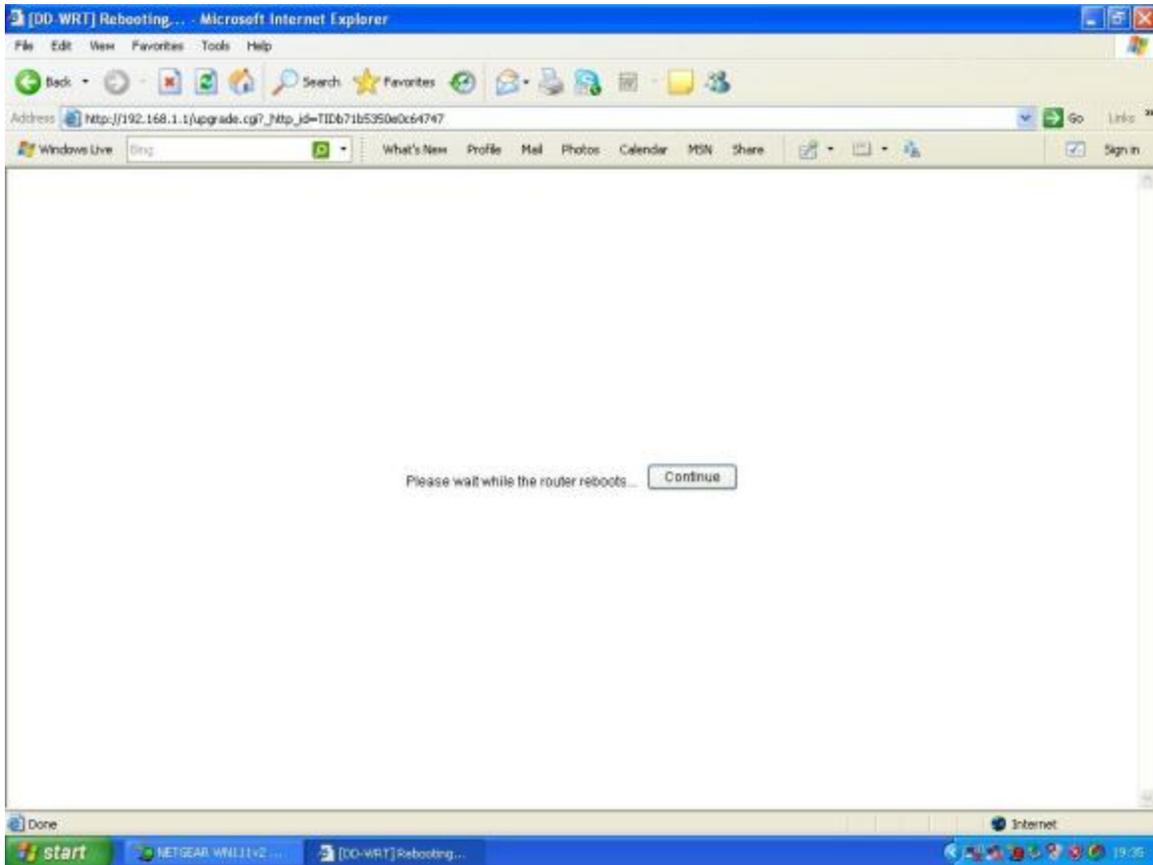
This will ask you for a confirmation as shown below:



Click OK to continue the flashing and this starts flashing process.



Once the flashing finishes successfully, it shows following page.



Click continue to proceed.

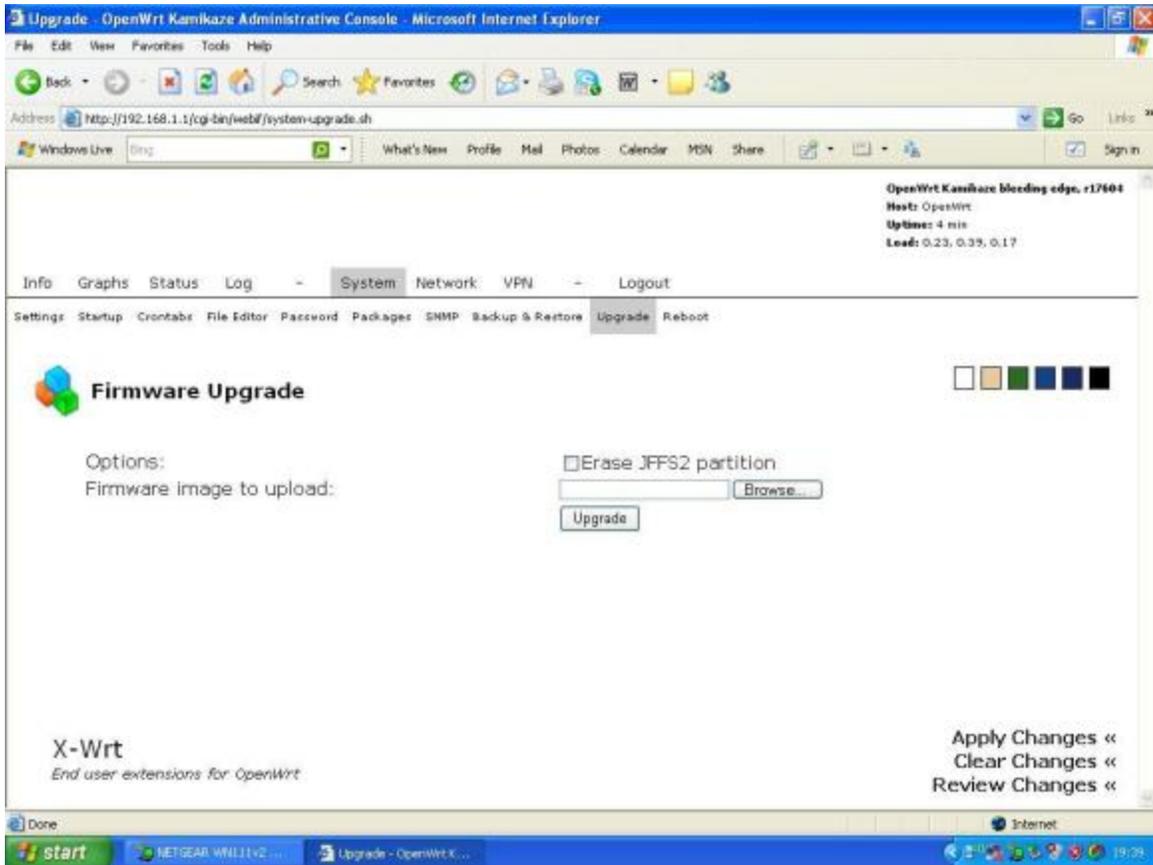
This is how firmware upgrade can be done from Tomato.

[[page]]

## **Firmware Upgrade from X-WRT:**

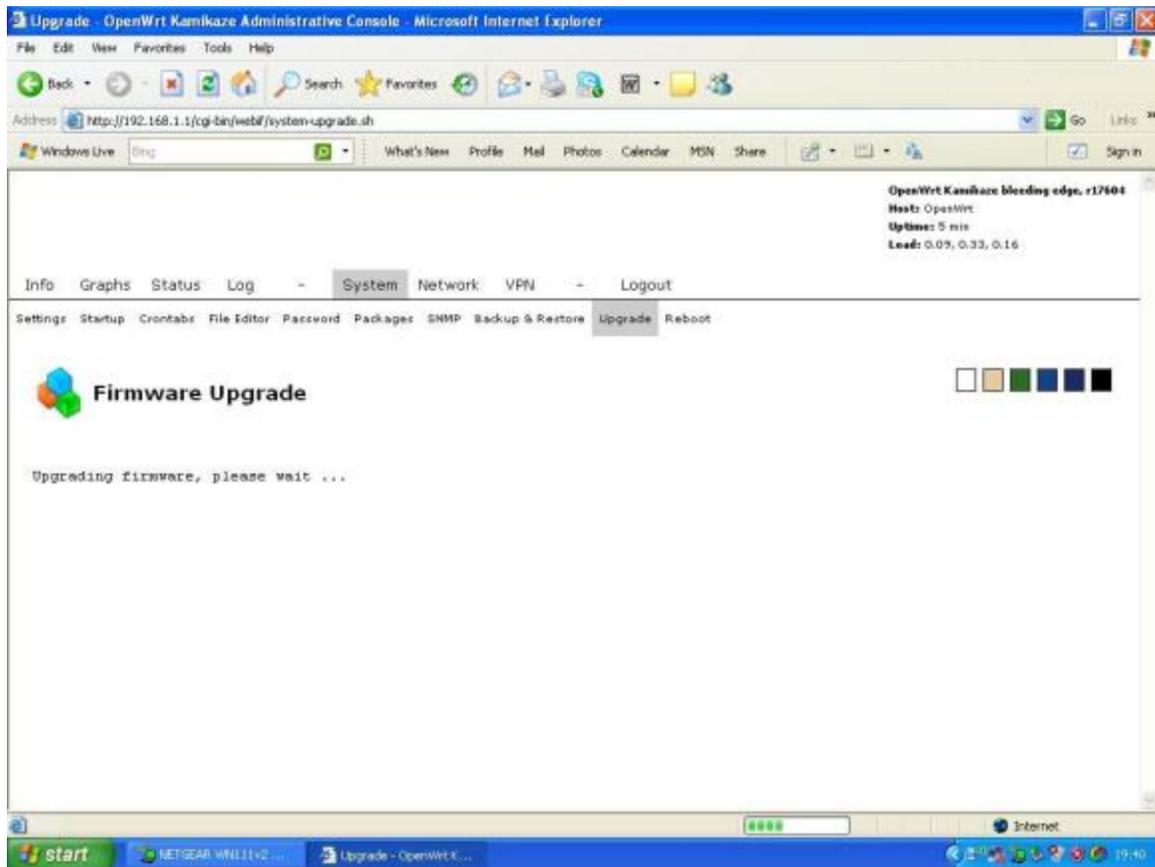
Firmware upgrade from Open WRT GUI (X-WRT) can be done using following steps:

Click the Upgrade tab under system tab which shows the firmware upgrade page as shown below:



Click browse to select the file to flash and then click upgrade to start upgradation.

Once upgradation starts you will see the following page:



OpenWRT does not provide any page to confirm completion of flashing process. Once flashing completes, the above page disappears. You need to enter the IP of your board into the browser to access its GUI.

NOTE : Do a hard factory reset whenever you do a firmware upgrade.

## Recovery process of the board:

A board may become dysfunctional due to various reasons and also the extent of this varies depending on the causes.

1. After doing a firmware upgrade one may not be able to access the board because of some mismatch in nvram parameters. In such cases a hard factory reset sets all nvram parameters to their default values for that particular firmware and the board becomes functional.
2. Due to a nvram mismatch, some features work while others don't work. For example, ping works but GUI access does not. In such cases, a hard factory reset solves the issue.
3. The flashed firmware has a wrong flash layout and in such cases, the boot process will repeat in cycles. If that is the case, the router is bricked and only way to recover is to set up a serial interface to access its console.
4. It may also happen that flashed firmware has a wrong board id and in such case also boot will

not happen. In such case one needs to give the following command at the console of the board:  
"burnboardid <>" (without quotes) Also for USB and Wireless to work simultaneously,  
boardflags should be 0x00000710.

## NVRAM Commands

Nvram commands can be used to set/get nvram parameters at board's console.

Their syntax is as follows:

```
nvram get <>
```

```
nvram set <>
```

## Flash Layout of Default WNR3500L Firmware

Flash layout specifies the offsets for different components of a firmware in flash.

It varies from firmware to firmware, but one should make sure that for WNR3500L first 4\*64K blocks are used for CFE and last two 64K blocks are used for board data and nvram respectively.

The flash layout for default NETGEAR firmware is as follows:

```
0x00000000-0x00040000 : "boot"  
0x00040000-0x00790000 : "linux"  
0x000d0f7c-0x00790000 : "rootfs"  
0x00790000-0x007a0000 : "ML1"  
0x007a0000-0x007b0000 : "ML2"  
0x007b0000-0x007c0000 : "T_Meter1"  
0x007c0000-0x007d0000 : "T_Meter2"  
0x007d0000-0x007e0000 : "POT"  
0x007e0000-0x007f0000 : "board_data"  
0x007f0000-0x00800000 : "nvram"
```

## Quick Links

- [WNR3500L Review](#)
- [WNR3500L Downloads](#)