Click here for **Page 1** of this wiki.

Contents

Overview Items

See Overview Items on page 1.

A Major Step Forward

See A Major Step Forward on page 1.

Differences in Hardware

See Differences in Hardware on page 1.

Support Threads

See Support Threads on page 1.

Firmware Repository

See Firmware Repository on page 1.

Third-party Developer FW

See Third-party Developer FW on page 1.

Which FW Image for Me?

See Which FW Image for Me? on page 1.

Flashing from Stock Asus FW to DD-WRT

See Flashing from Stock Asus FW to DD-WRT on page 1.

Updating DD-WRT

See Updating DD-WRT on page 1.

Mounting File System for External Storage

See Mounting File System for External Storage on page 1.

Mount FS by Direct Access Method

See Mount FS by Direct Access Method on page 1.

Mount FS by Download Method

See Mount FS by Download Method on page 1.

Automounting ext3/FAT/FAT32/NTFS

See Automounting ext3/FAT/FAT32/NTFS on page 1.

Installing Optware Light

See Installing Optware Light on page 1.

Installing a Transmission-daemon onto Asus RT-N13U

I have just successfully installed and running this Transmission Torrent thingy

and thanks to "Gouryella" for showing us the light

adopted with slight Modification from Transmission daemon kudos to anonymous code-angels--Capper 22:07, 25 August 2010 (CEST)

1. Make the following folders

```
cd /opt
mkdir -p /opt/data/torrents/.config              # -p to make directories at the same time
```

The plan is to have everything torrent go to the folder /opt/data/torrents

2. Install Optware Transmission

```
/opt/bin/ipkg-opt -verbose_wget install transmission
```

> Note: I like to see the progress of the downloading process, so I know the right thing is happening. This is done with the -verbose_wget parameter.

3. Started and stopped Transmission to get the basic work folders

```
/opt/bin/transmission-daemon -g /opt/data/torrents/.config/transmission-daemon
killall transmission-daemon
```

With the command above you get the basic folder structure of:

```
/opt/data/torrents/.config/
/opt/data/torrents/.config/transmission-daemon
/opt/data/torrents/.config/transmission-daemon/settings.json  #file
/opt/data/torrents/.config/transmission-daemon/blocklists
/opt/data/torrents/.config/transmission-daemon/resume
/opt/data/torrents/.config/transmission-daemon/torrents
```

4. Edit *settings.json*

```
nano /opt/data/torrents/.config/transmission-daemon/settings.json
```

5. Delete contents of *settings.json* and copy-paste following code into it.

```
{
"blocklist-enabled": 1,
"download-dir": "\/opt\/data\/torrents",
"download-limit": 100,
"download-limit-enabled": 1,
"encryption": 2,
"max-peers-global": 35,
"peer-port": 25000,
"pex-enabled": 1,
"port-forwarding-enabled": 1,
"rpc-authentication-required": 0,
"rpc-password": "",
"rpc-port": 9091,
"rpc-username": "",
"rpc-whitelist": "192.168.1.*",
"upload-limit": 200,
"upload-limit-enabled": 1
}
```

The file *settings.json* can also be downloaded from here (the wget command is one line):

```
wget http://www.3iii.dk/linux/optware/settings.json -O /opt/data/torrents/.config/transmission-d
```

but change to "download-dir": "\/opt\/data\/torrents", from "download-dir": "\/mnt\/data\/torrents",

6. Open listening port for WAN access

Go to your DD-WRT control panel and add the following to Administration - Commands - Firewall

```
iptables -t nat -I PREROUTING -p tcp -d $(nvram get wan_ipaddr) --dport 25000 -j DNAT --to 192.16
iptables -I INPUT -p tcp -d 192.168.1.1 --dport 25000 -j logaccept
```

You may change the value 25000 to whatever port you specified in the settings.json file for the value "peer-port"

7. Restart transmission

```
/opt/bin/transmission-daemon -g /opt/data/torrents/.config/transmission-daemon
```

8. Accessing Transmission web interface

Now you get web access to the Transmission page by going to **http://192.168.1.1:9091**. That is, if your routers IP is 192.168.1.1

9. Autorun Transmission-daemon every time router reboot

I would not like to go to command shell and type to start the Daemon. so here is the autostart for couch potatoes like me.

```
cd /opt/etc/init.d
rm S99trans
```

This will remove old S99trans initializing file you might have in the directory . We will now create an autorun script for our Transmission-Daemon

```
nano S99trans
```

now type-in following lines in it

```
sleep 120
/opt/bin/transmission-daemon -g /opt/data/torrents/.config/transmission-daemon
```

Save it by presseing CTRL+O followed by CTRL+X , now we will Make it executable by...

```
chmod +x /opt/etc/init.d/S99trans
```

You are done. Enjoy downloadig sans PC.

10. How to get transmission to download torrent files?

```
- In a web browser go to your favourite torrent site/tracker and download a "<myfile>.torren
- In a web browser go to 192.168.1.1:9091 to enter the Transmission web page.
- click "open"
- click the text field (or "select" button)
- point out the "<myfile>.torrent"
- click "upload"

and the torrent'ed file should start downloading shortly.
```

The downloaded file will turn up in the **/opt/data/torrents** folder.

The full space of the file will be reserved from the start, so in a FTP, WinSCP or Explorer via Samba it may seem like the file is all there immediately, but it is not! It is fully downloaded when the line turns green in the Transmission web interface at *192.168.1.1:9091*.

You can see details about any of the torrent files by clicking the Inspector button on the right in the Transmission web interface.

11. Another interface option

You might also want to check out a front-end (remote-GUI) for the rpc version of transmission.

transmission-remote-gui is an application written in Free Pascal to remotely manage Transmission See: http://code.google.com/p/transmisson-remote-gui

transmission-remote-dotnet is a .NET application written in C# to remotely manage Transmission. See: http://code.google.com/p/transmission-remote-dotnet/

"Try the latest one (beta is welcomed over here)"

Installing a Network Printer onto Asus RT-N13U

As of v24-PreSp2 (first versions to work on Asus RT-N13U) jffs was removed due to the lack of space available. However, Brainslayer put the support of network printing onto the firmware, enabling use of a network printer. Special Thanks for TimeKiller for figuring out most of the solution.

1. First enable USB support

Enable the following under Services -> USB:

```
Core USB Support
USB 1.1 Support (UHCI)
USB 1.1 Support (OHCI)
USB 2.0 Support
USB Printer Support
```

2. Startup Settings

Go to Administrations -> Commands, and add this:

```
sleep 4
mkdir -m 755 -p /dev/usb
mknod -m 660 /dev/usb/lp0 c 180 0
/usr/sbin/p910nd -f /dev/usb/lp0 1
```

Save on the Startup.

3. Reboot and Install Drivers

Reboot the router, then install drivers through tcp/ip (9101)

For Windows 7:

```
Go to Devices and Printers
Then, press Add a Printer
Got to Network Printers
Skip the detection, as Windows will not find anything
Go to "Add a printer using a tcp/ip address or hostname"
Device type: Autodetect
Hostname and ip address: your router's ip (default 192.168.1.1)
Port Name: Anything (puts your router's ip by default)
After it says it could not detect a printer, select custom, then Advanced
Make sure the protocol is RAW and change the Port Number is 9101
Install your drivers and finish.
```

You should print a test page to see if it works.

4. Troubleshooting If the test page does not come, try these settings instead:

Go to Administrations -> Commands, and add this:

```
sleep 4
chmod +rwx /usr/sbin/p910nd
mkdir -m 755 -p /dev/usb
mknod -m 660 /dev/usb/lp0 c 180 0
chmod +rwx /dev/usb/lp0
/usr/sbin/p910nd -b -f /dev/usb/lp0 0
```

Save again on the Startup. Reboot then follow the steps above but instead of port 9101, put in 9100. You should print a test page again to see if it works. If it doesn't work, you somehow did not follow the instructions correctly.

Fire up a Second Wireless Network w/ Optional Bandwidth Throttling

A second (or even third) wireless network (WLAN, VLAN) is useful for sharing the router's Internet connection. New wireless networks are easily configurable:

- Secure (private) or open (hotspot)
- Complete or partial isolation from the main network
- Unique SSID
- Variable bandwidth alloted by optional QoS settings

These instructions use only the web interface (noob-friendly) and should work for any router running DD-WRT.

Browse to the router's home page and login, then:

1. Create Virtual Interface for New Wireless Network

On Wireless | Basic Settings page, under 'Virtual Interfaces' click **Add**

- Key second SSID, the 'Wireless Network Name' preferred, Ex. BobNet, YoHotspot.
- Check that 'Wireless SSID Broadcast' is **Enable**
- Set 'AP Isolation' as preferred: **Enable** (default) for client-to-client communication on the new wireless network, **Disable** to isolate each.
- Set 'Network Configuration' to **Bridged**
- Be sure 'Wireless Mode' at top of page is set to **AP** (Access Point)
- Click **Apply Settings**.

2. Set Security for New Wireless Interface

On the Wireless | Wireless Security page, under 'Virtual Interfaces ra1 SSID...' ("ra1" is the new wireless interface just created in step 1.), set parameters as desired for security. These setting work exactly the same as

for the router's physical interface (shown at top of page), but apply only to the new wireless network.

- For public access/hotspot, 'Security Mode' would be **Disable**.
- A shared secure network would normally use **WPA2** and **AES**.
- When done, click **Save**.

3. Create Bridge for New Wireless Interface

On the Setup | Networking page, under 'Bridging' click **Add**.

- In leftmost (unlabled) field that pops up, key "**br1**" (without quotes),
- Set 'STP' to **Off**, and
- Leave 'Prio' (Priority) and MTU as they are. Click **Save**.
- New fields will appear for 'IP Address' and 'Subnet Mask'. Populate these (Typical values might be 192.168.**16**.1 and 255.255.255.0, used in following examples.) and click **Save**.
- Reboot.

4. Assign New Wireless Interface to New Bridge

Still on Setup | Networking page, under 'Assign to Bridge' click **Add**. On Assignment line that appears:

- Select '**br1**' in dropdown menu,
- Pick '**ra1**' in second dropdown menu (labeled 'Interface'),
- Set priority, 'Prio', as desired. Higher number = lower priority. The corresponding priority numbers (under 'Create Bridge' and 'Assign to Bridge') should be similar. Ex. 32768 and 32760.
- Click **Save** and reboot.
- Check in 'Current Bridging Table' that ra1 interface is assigned to br1 (they appear on same line). If not, edit any bad entries, possibly Delete and re-key, **Save**, reboot, and repeat this step.

5. Enable DNSMasq as Sole DHCP Server

This has the added benefit of running the router more efficiently*. On Setup | Basic Setup page, see that:

- 'DHCP Type' is **DHCP Server**
- 'DHCP Server' is **Enable**
- 'Use DNSMasq for DHCP' is **checked**
- 'Use DNSMasq for DNS' is **checked**

On Services | Services page, set:

- 'Used Domain' to '**LAN & WLAN**"
- 'LAN Domain' to some name (Ex. **mylan**, yourlan, lan1, alan etc.)
- 'DNSMasq' to **Enable**
- 'Local DNS' to **Enable**
- In 'Additional DNSMasq Options' window, paste the following:

```
local=/mylan/
expand-hosts
```

```
interface=br1
dhcp-range=br1,192.168.16.100,192.168.16.120,255.255.255.0,1440m
```

- Edit the above pasted text to customize as needed:
  - ♦ Replace "mylan" with the name chosen for 'LAN Domain' if different; these must match.
  - ♦ Edit the "120" -- which allows 20 clients to connect simultaneously -- as desired.
  - ♦ Edit both occurrences of "192.168.16." to match the address keyed in 'Create Bridge for New Wireless Interface', above.
- Click **Save** and reboot.

*(For details, see DNSMasq page.)

6. Set Level of Isolation for New Wireless Network

Unless the new network is secure and all connected clients trusted, some isolation is needed.

- The easiest setup completely isolates the new network -- its clients have full access to the Internet, but not to the router or its wired or wireless clients. On the Administration | Commands page, under 'Command Shell', paste the following into the 'Commands' window:

```
iptables -I FORWARD -i br1 -o br0 -j DROP
iptables -I INPUT -s 192.168.16.0/24 -d 192.168.1.0/24 -j DROP
```

- As above, edit the subnet addresses, 192.168.16 and 192.168.1, if customized. Click **Run Commands** and test/verify that everything works as expected. All pings or other attempts to connect between the two subnets should fail. Reboot if any problems.
- When satisfied, with final iptables rules in 'Commands' window, click **Save Firewall**. Note: A click of this button with bad rules showing can lock everyone out of the router, necessitating a hard reset (and loss of all custom settings). Do not skip the previous test step.
- If instead of total isolation it is desired to grant partial access to new networks' clients, determine which rules to modify and use (Ex. below), test and save as above.

```
iptables -I INPUT -i br1 -p tcp --dport www -j REJECT
iptables -I INPUT -i br1 -p tcp --dport telnet -j REJECT
iptables -I INPUT -i br1 -p tcp --dport ssh -j REJECT
iptables -I INPUT -i br1 -p tcp --dport https -j REJECT
```

7. Set Bandwidth Limits on New WLAN (Optional)

The maximum bandwidth taken by the new wireless network can be limited by following these steps. New WLAN clients will otherwise compete for bandwidth on equal footing with those on the main network.

- Navigate to one or more speed test sites (Ex. Speakeasy) and note maximum Up- and Down-link speeds.
- On NAT/QoS | QoS page, enable QoS ('Start QoS' **Enable**) and check that 'Port' is **WAN** and 'Packet Scheduler' is **HTB**.
- In 'Uplink' and 'Downlink' fields, key desired maximum throttled values in light of speed test results above. To convert, Ex. 5.8 Mbps from test=5800 kbps, and 0.57 Mbps=570 kbps.
- Note: Settings below will make the throttled speeds just entered ('Uplink'/'Downlink') apply only to the new wireless network. While the help screen sets a guideline of "80%-100%" of maximum, these

throttled values can be set to whatever the admin desires, perhaps as low as 10%. A setting of 50% could prove perfectly functional. Performance testing and tweaking is recommended.

- Under 'Netmask Priority', key new wireless subnet address. Using same as above, 192.168.16.0(/)24. Click **Add**.
    - ♦ On the line that appears, set 'Priority', Ex. **Bulk**. Click **Save**.
- Repeat for main interface (Ex. 192.168.1.1(/)24), click **Add**, set priority as desired, typically '**Exempt**', click **Save**.
- Reboot.

Note that throttling can also be applied based on application Service or MAC address.

If all steps were followed, the second SSID should appear to wireless clients in the area, their login and connection subject to the security and bandwidth settings made here. It is good to share with thy neighbor!

Sound Card

Sound works great. (#full post on the way, not done yet#)

DLNA/UPnP Media Servers

Unfortunately, the firmware for this router suffers from the same affliction as all factory K26 builds, explained in this thread. Essentially, no DLNA/UPnP media server will run, and no Kong mod releases (which fix the problem) are yet available for Ralink devices.

Perhaps one of our local experts will apply the patch (and include miniDLNA, like the Kong mod). Or maybe the factory firmware will be corrected. Until such time, attempts to run media servers like uShare will be fruitless.

For B1:facsi posted on this this thread, a solution using RT-n56u package.

After optwares was installed do:

ipkg install http://rt-n56u.googlecode.com/files/minidlna_1.0.24-1_mipsel.ipk

MiniDLNA's configuration file is located at /opt/etc/minidnla.conf

The network_interface needs to be changed to the appropriate one, br0.

network_interface=br0

Set your media share directories. content is defined by a preceding A(audio), V(video) and P(picture). Keep in mind that Linux is a case-sensitive OS.

media_dir=V,/mnt/share/Videos

media_dir=P,/mnt/share/Pictures

media_dir=A,/mnt/share/Music

Set your friendly name to whatever you want.

friendly_name=Media Server

If you have a large library and want your library database kept between program runs, you MUST change this setting. If you aren't hosting many files, or don't mind it rebuilding every reboot, you can leave this the same.

db_dir=/mnt/tmp/minidlna

Set inotify to watch for new files to be added to the library. Inotify searches for new files every 60 seconds.

inotify=yes

Enabling Tivo support and strict dlna is by user preference.

enable_tivo:nostrict_dlna:no

This is important: CHANGE the presentation url or your devices will not see the server. Set it to your router's IP address with 8200 port.

presentation_url=http://192.168.1.1:8200/

Set the notification interval and model numbers to whatever you want.

minidlna.conf file looks like:

port=8200

network_interface=br0

media_dir=A,/mnt/share/Music

media_dir=V,/mnt/share/Videos

media_dir=P,/mnt/share/Pictures

friendly_name=Media Server

db_dir=/mnt/tmp/minidlna

album_art_names=Cover.jpg/cover.jpg/AlbumArtSmall.jpg/albumartsmall.jpg/
AlbumArt.jpg/albumart.jpg/Album.jpg/album.jpg/Folder.jpg/folder.jpg/Thumb.jpg/thumb.jpg

inotify=yes

enable_tivo=no

strict_dlna=no

presentation_url=http://192.168.1.1:8200/

notify_interval=900

serial=12345678

model_number=1

Device Specifications

- Power Supply = 12VDC 1,0A
- Ethernet Ports = 1x WAN RJ-45 10/100 Base T, 4x LAN RJ-45 10/100 Base T
- Antennas = 3x internal antennas
- USB ports = 1x USB2.0
- Wireless standards supported: 802.11b (max. 11 Mbit/s), 802.11g (max. 54 Mbit/s), 802.11n (max. 300 Mbit/s, 2.4 GHz only)
- RAM = 32 MB (64 MB in rev B1)
- Flash = 4 MB (8 MB in rev B1)
- CPU = Ralink RT3052F clocked at 384 MHz

Authors

- gouryella: Automounting ext3/FAT/FAT32/NTFS (download FS method), Installing Optware Light
- ZenKen: started wiki, Specifications, early flashing guide, gouryella's optware guide
- Capper: Installing a Transmission-daemon onto Asus RT-N13U
- MicroClue: Installing a Network Printer onto Asus RT-N13U
- u2n: Introduction, Overview Items, Flashing from Stock Asus FW to DD-WRT, Updating DD-WRT, Mounting File System for External Storage, Mount FS by Direct Access Method, Fire up a Second Wireless Network w/ Optional Bandwidth Throttling, Sound Card, DLNA/UPnP Media Servers, Authors