English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Be aware that there are two versions of Optware. This page is for information OTRW (frater).

if you are looking for OTRW2 please go here

Prerequisites

Optware runs on **Broadcom routers only**. The installer script only works on Kernel 2.4 & 2.6 (K24 & K26).

The following builds are supported:

```
* BrainSlayer builds up to 19519
* Fractal builds up to 20006
* All Kong builds based on Kernel 2.6

* Kong AC builds are not supported
```

Contents

== **Frater's no hassle, newbie friendly Optware** == (Donation possible)

This is the latest, greatest and easiest way to enable Optware on your Router. It is **recommended** that you have a router with USB capable storage (Harddisks (must be self-powered), flash-drives etc.) and the **LATEST** build! (preferably freshly flashed)

For BrainSlayer builds. Common routers use broadcom or broadcom k26. Choose the appropriate newest build, then navigate the directories.

For Eko Builds, K26 here All Others Here

The SD/MMC Method is working thanks to DHC Darkshadow. **For USB users, you wont be needing JFFS2, so DISABLE it!** Another aspect to note is that some of these services (i.e Twonky) consume alot of CPU resources, so make sure you check your resource consumptions.

Default Services that will be installed:

- **Bash instead of shell in busybox** - (LFS support)
- **Automounting, Unmounting and Hotmounting of storage devices** - Automatically mounts all recognized partitions and filesystem formats (including NTFS in K26).
- **Network printing with Watchprinter** - Plug a USB printer into your router and let anyone on the LAN (or even WAN) print.
- **Torrent transmission with watchdog** - Including Bittorrent transmission with Web Administration
- **Pre-configured Samba share** - Samba provides file and print services for various Microsoft Windows clients and can integrate with a Windows Server domain, either as a Primary Domain Controller (PDC) or as a domain member. http://www.samba.org/
- **NFS File Sharing** - It is now possible to share files via NFS in a pure Linux environment.
- **Portmap** - Used in conjunction with the NFS Daemon. More information regarding what it does and how to implement NFS can be found here: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=85211
- **Xinetd** - A replacement for inetd, the internet services daemon. Controls user defined network services such as printing and SWAT (Samba Web Administration Tool) http://www.xinetd.org/
- **Pound** - A lightweight open source reverse proxy program suitable to be used as a web server load balancing solution. http://www.apsis.ch/pound/
- **Asterisk** - A software that allows you to set up a voice communications server. http://www.asterisk.org/

- **Lighttpd** - A fast webserver with minimal memory footprint. http://www.lighttpd.net/
- **Vlighttpd** - Allows you to get a 2nd IP on your system and run virtual hosting there.
- **Pixelserv** - A super minimal webserver, it's one and only purpose is serving a 1x1 pixel transparent gif file. Using some creative firewalling (netfilter/iptables) rules you can redirect some webrequests (for adds for example) to pixelserv. http://proxytunnel.sourceforge.net/pixelserv.php
- **AsiaBlock** - A custom iptables firewall that is configurable to block certain countries from accessing your Webserver, FTP or just general Web surfing.
- **Worldblock** - Very similar to Asiablock, other than the fact that it is for blocking everything except your country. To properly use this service, you must know how to use Vi editor to add your country.
- **StopHack** - This CRON script will check /var/log/messages for pound entries that are malicious and put the IP's in /opt/etc/asia.spam. The AsiaBlock service MUST be running for this to work.
- **Stophammer** - Similar to stophack, only it provides firewall services that increase your network security in a very respectable fashion. See Service examples below to understand how it works.
- **Vim with proper terminal support** - Vim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', with a more complete feature set. http://www.vim.org/about.php
- **Twonky Media** - Share your media on compatible devices throughout your home. http://www.twonkymedia.com/
- **Siproxd** - A masquerading SIP Proxy Server. Siproxd is a proxy/masquerading daemon for the SIP protocol. It handles registrations of SIP clients on a private IP network and performs rewriting of the SIP message bodies to make SIP connections work via an masquerading firewall (NAT). It allows SIP software clients (like kphone, linphone) or SIP hardware clients (Voice over IP phones which are SIP-compatible).
- **News Server (Nzbget)** - A command-line client/server based binary newsgrabber for nzb-files. http://nzbget.sourceforge.net/Overview
- **Fixtables** - This service is used to fix a firewall rule-set bug that is present in all K26 firmwares. K24 is not affected. The service also contains **VITAL** security measures against current DD-WRT builds! It is highly recommended to use.
- **Zabbix** - Zabbix offers advanced monitoring, alerting and visualization features today which are missing in other monitoring systems, even some of the best commercial ones. This service blows away SNMP, Cacti, Wallwatcher, etc. For more information, search the forums and check out the website! http://www.zabbix.com/features.php
- **Reloc_syslogd** - A service that is designed to extend the size of DD-WRT's syslogd and integrate kernel logging into */opt/var/log/messages*
- **Service tool** - Control all of these services. (Usage explained below)
- Services running as other users than root

- Other various useful tools such as net and storage diagnostics..

In my opinion, **Everyone** with a router that has **storage device capabilities** should take advantage of this! You will NOT regret it, even if it can be a time consuming process! If you are worried about formatting to a Linux filesystem and it's compatibility with windows, check out this thread from the forum on using the Windows NT Filesystem (NTFS)!

Getting Started

```
****  This method does NOT support Atheros based routers. ****
```

If you do not know if your router is Broadcom or Atheros then ... If you want ipkg for these type of Atheros routers see this thread.

These routers have been verified with Optware. If you have had success, please edit this section and add your model and name (add your name if model is already listed):

- Asus RT-N16 (gatorback)
- Linksys E3000 / E4200v1 (basmaf)
- WRT N600 (lost-in-space)

If starting from scratch, you will need to first format and partition your harddisk (ext2 or ext3), flashdrive or SD card (ext2 **ONLY**) Linux filesystem. **Ext2 should be used for flashdrive because it does not use journaling (like ext3).** It is much easier than you think, and can be accomplished via a Linux Live boot-CD: sysrescuecd: gparted utility. There will be NO changes to your PC whatsoever, and it is very quick to implement.

[gatorback]: In the WL-520GU (4MB firmware) only ext3 is supported, however a module ext2.o can be inserted in the kernel at bootup. Module and details are published here: [1] The WL-520GU does not have enough hardware to support a typical OTRW install.

Drive Preparation and Prerequisites

Before you can utilize this extremely beneficial addition to your USB capable router, you must follow these important instructions:

How to - Format and Partition External Storage Device

This **must** be done for Optware to work correctly!

Connecting the Drive to your Router

NOTE:

The are reports of flash drives that do not work: [2]

For users with small /opt partitions (**Less** than **256MB**, such as flashdrives and SD/MMC cards) use this as your start-up script:

```
mount -o noatime -t ext3 /dev/scsi/host0/bus0/target0/lun0/part1 /opt
```

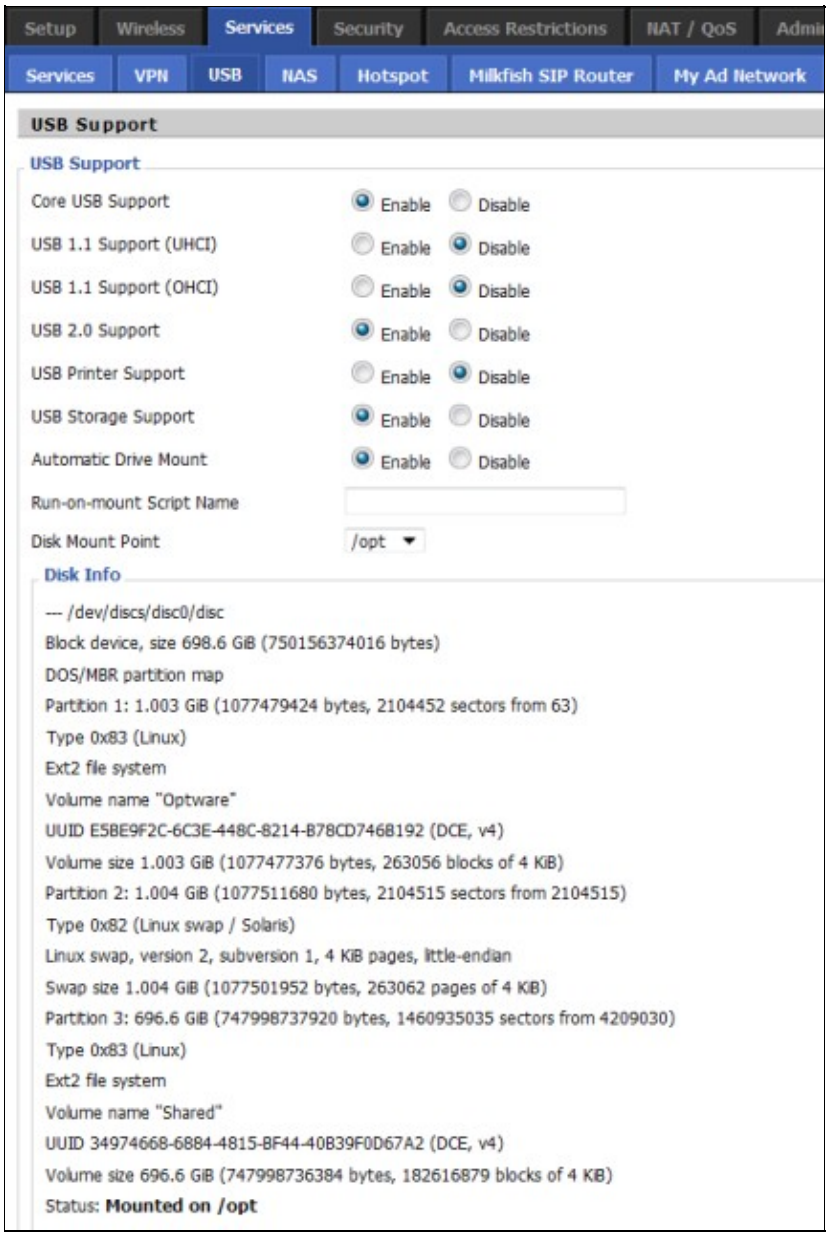
For external HardDrives, use the following method:

1. In the DD-WRT web GUI screen, on the Services USB tab enable the options for:

- Core USB support
- USB 2.0 support (**Asus WL520gU routers** must use USB 1.1 drivers only!)
- USB storage support
- Printer Support (optional)
- ext2/ext3 File System support - Only for builds older than SVN 15501 !! The new system automatically selects FS type.
- FAT File system support (optional, but try enabling this if your USB won't mount, even if you aren't using FAT FS) - Only for builds older than SVN 15501 !! The new system automatically selects FS type.
- Automatic Drive Mount

- In the **Disk Mount Point** drop-down menu, mount to **/opt**

2. From the DD-WRT web GUI screen, click on **Save Settings**, then **Apply Settings** 3. If everything was done correctly, this should appear on your **Services -> USB** Tab:



IMPORTANT

If using a USB hub to connect multiple devices, make sure NOT to overload the routers power supply. If the devices are self-powered, still be careful. Flashdrives do consume quite a bit of power, and even the I/O of the self-powered devices pulls some current.

Executing the Script

Start a terminal session using telnet or SSH

To do this in Windows, go to Start -> Run and type the following:

telnet 192.168.1.1 (use the ip address of your router if different than 192.168.1.1)

Enter the following at the telnet prompt:

login:**root**

password: **router's admin password to the web interface**.

NOTE When entering your password, the characters will **not** show up. This is normal for security. If it doesn't work the first time, make sure you don't make a typo or that the caps lock is not on when entering it.

See also: Telnet/SSH_and_the_Command_Line

In Windows, telnet can be accessed from a command prompt... **Start ->Run**, while a program like PuTTY will allow for either telnet or SSH sessions and is a much more flexible and secure shell prompt. It does not even need to be installed..

NOTE - Can't login via SSH

If you find that you can't log in to SSH after installation, check that you're using a build greater than, and including 12827. The reason is that bash is used as shell after installation, but older firmware builds don't allow for shells other than /bin/sh to be used in SSH.

Once logged in:

Issue the command **mount** to **ensure /opt** is mounted (K24 and K26 have different Device paths, observe the following; #1 is **K24** #2 is **K26**):

```
root@DD-WRT:~#mount
rootfs on / type rootfs (rw)
/dev/root on / type squashfs (ro)
none on /dev type devfs (rw)
proc on /proc type proc (rw)
ramfs on /tmp type ramfs (rw)
devpts on /proc/bus/usb type usbfs (rw)
/dev/scsi/host0/bus0/target0/lun0/part1 on /opt type ext2 (rw,noatime)
root@DD-WRT:~#
```

```
root@DD-WRT:~# mount
rootfs on / type rootfs (rw)
/dev/root on / type squashfs (ro)
none on /dev type devfs (rw)
proc on /proc type proc (rw)
ramfs on /tmp type ramfs (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw)
devpts on /proc/bus/usb type usbfs (rw)
/dev/discs/disc0/part1 on /opt type ext2 (rw,noatime)
root@DD-WRT:~#
```

Make sure you are able to connect to the internet through the router. Pinging a domain is a good example:

ping yahoo.com (or any other domain of your choice)

You should get a multi-line response along the lines of:

```
PING yahoo.com (72.30.2.43): 56 data bytes
64 bytes from 72.30.2.43: icmp_seq=0 ttl=52 time=106.551 ms
64 bytes from 72.30.2.43: icmp_seq=1 ttl=52 time=102.864 ms
64 bytes from 72.30.2.43: icmp_seq=2 ttl=52 time=101.219 ms
64 bytes from 72.30.2.43: icmp_seq=3 ttl=52 time=100.507 ms
64 bytes from 72.30.2.43: icmp_seq=4 ttl=52 time=96.661 ms
```

Once you see a few lines of that, hit **CTRL+C** to return to a root prompt.

If you do NOT see output as mentioned above, you need to troubleshoot to establish an internet connection first. Some possibilities:

A) Reboot the router. (this alone may help. If not, continue to suggestion B)

B) Power off your cable modem, then the router.
Wait 30 seconds, then power on the cable modem.
Wait 30 seconds and power on the router.
Wait 30 seconds, then telnet back into the router and repeat the ping test demonstrated above.

Now you should have a connection. If so, continue with the following steps.

Enter the following commands into Busybox/Telnet:

```
wget -O /tmp/prep_optware http://wd.mirmana.com/prep_optware
sh /tmp/prep_optware

Upgrade Command is the same
```

This will load all the necessary Optware and supporting scripts that Frater wrote from the ground up.

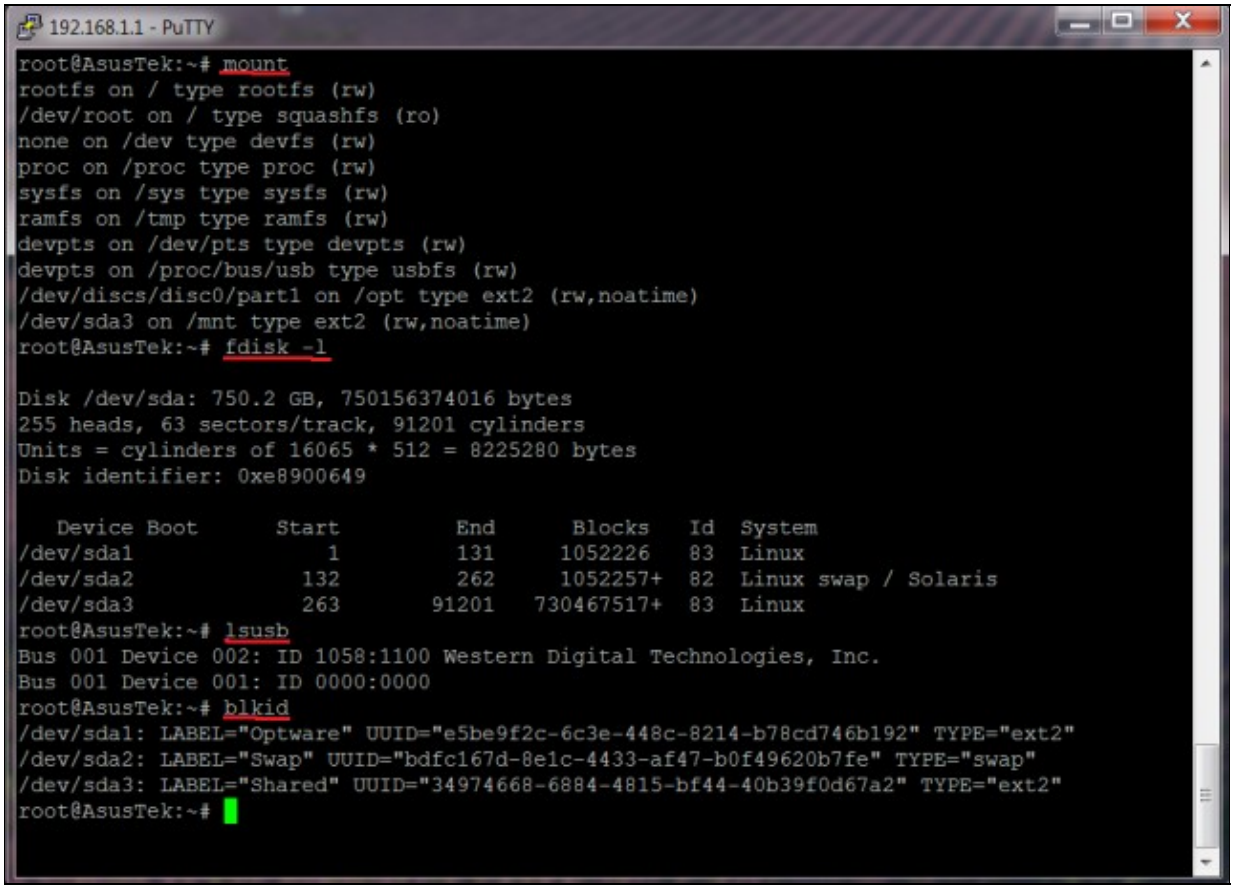
This will take about 10-20 mins depending on your connection and your router CPU clock. Close your Web Interface as this consumes precious memory and CPU resources

Once everything has completed, wait you will be returned to a root prompt. Wait a **minimum of 1 minute**, then type **reboot** into either the BusyBox/Telnet Shell (why not, you're right there) or reboot via Web Interface.

Important After rebooting, wait again at **least another minute** before logging back into the Telnet/SSH session!

Ensure Partitions are mounted

In either telnet or SSH, enter the command **mount** , or the other commands underlined in red , if everything is working properly, it should look like this:

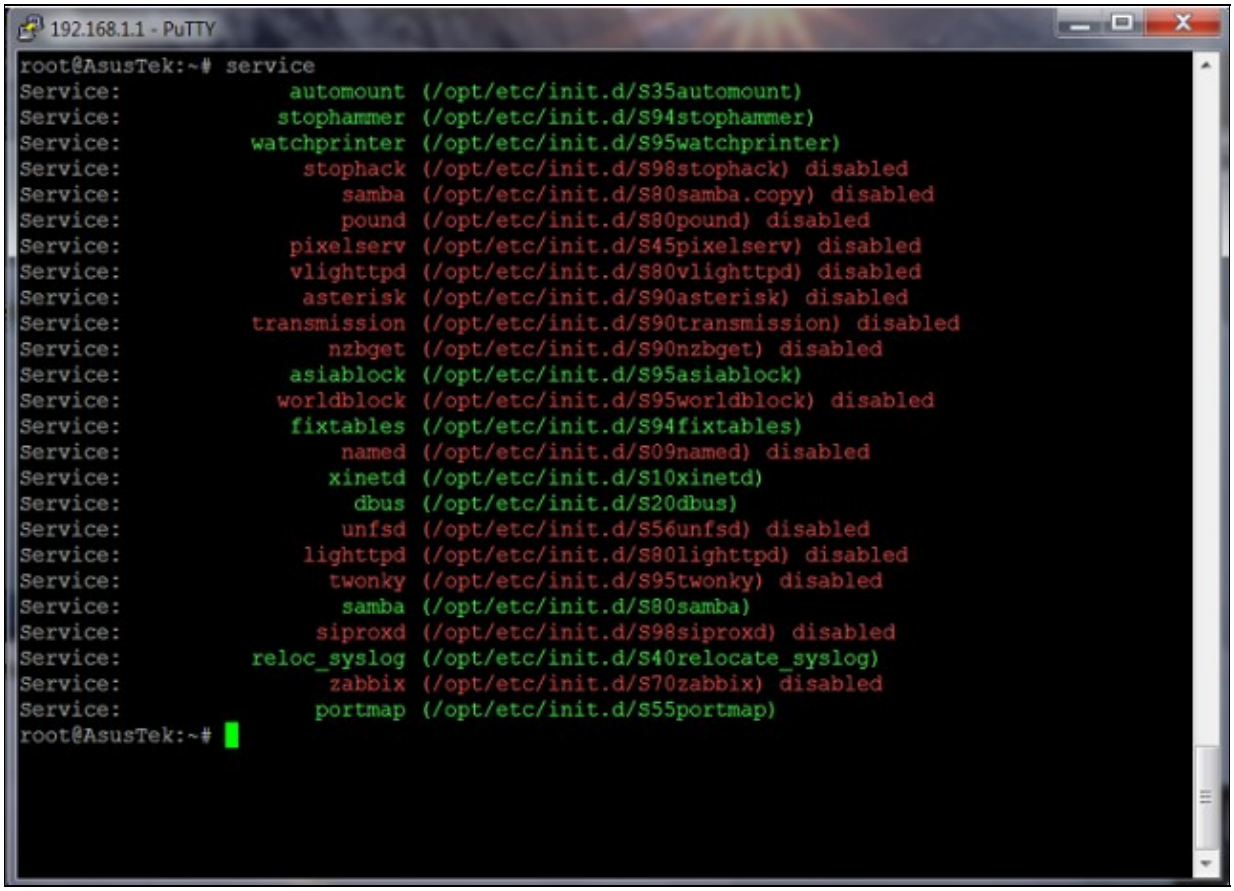


Important To keep track of your drives free space, issue the command **df -h**

You will get an output like this:

```
root@Asus:~# df -h
Filesystem            Size  Used Avail Use% Mounted on
rootfs                5.7M  5.7M     0 100% /
/dev/root             5.7M  5.7M     0 100% /
/dev/discs/disc0/part1
                      756M  215M  534M  29% /opt
/dev/sda4             293G  173G  117G  60% /mnt
/dev/sda3             504M   17M  483M   4% /tmp/c
root@Asus:~#
```

Using PuTTy to enable/disable Services



BusyBox/Telnet Commands for services:

```
service - show all services (enabled/disabled)
service <service name> - if "status" parameter is supported, will show service status, otherwise
service <service name> on - Enable the script, allowing execution (chmod +x  /opt/etc/init.d/S<se
service <service name> off - Disable the script, disallowing execution (chmod -x  /opt/etc/init.d
service <service name> start - Start/execute the script, as long as service is enabled (i.e. perm
service <service name> stop Stop/kill the script, if the service is running
service <service name> restart Stop/kill the script, if the service is running, and then start/ex
service <service name> <parameter> - Run the script with the parameter.
```

For a service to work it must be first switched **on***, and then told to **start**.

```
service <service name> on
service <service name> start
```

- Once you enable a service with the **on** parameter, the service is set to allow execution, and will run the next time you restart your router. You will need to issue a **start** directly proceeding it to initiate the service if you wish to start the service without restarting your router. A service must be set to on before it can be started.

Examples:

```
service xinetd status
service xinetd off
service xinetd on
service xinetd start
service xinetd stop
service xinetd restart
```

NOTE Xinetd will need to be started after the optware has been installed and the router has rebooted.

Issue:

```
service xinetd on

service xinetd start
```

This service MUST be enabled for services such as **Network Printing**, **SWAT** (web admin/config for samba) and **OpenVPN**

Turning off Twonky

Twonky Media Server (google it) may be enabled by default. It is a massive resource hog and can bog down even the most powerful routers. It is recommended to disable it unless you require its services.

```
service twonky stop
service twonky off
```

Automount

```
service automount start - mount all partitions
service automount stop - umount all partitions instead of the one to /opt
service automount status - show all partitions
service automount umount <partition|mountpoint> - unmount that partition and remove it fromautomo
service automount nomount <partition> - Do not automount this partition
service automount nonomount <partition> - remove this partition from the nomount list
```

Upgrading to Samba 3.5

If you wish to remove the default Samba service (Samba 2), which is incompatible with Windows Vista and 7, and you have the necessary hardware resources, Samba3 is a good tutorial to follow.

See NOTES at the bottom of this page for important/useful commands

Service Explanations/Configuration Examples

BackupEssential

- **Backup/Restore on Different Hardware**- This allows you to backup your settings on one router, change builds, and then restore the settings without having to reconfigure by hand (using DD-WRT's Web GUI method is NOT safe, other than this method).

Telnet or SSH into your router. Type "backupessential" and **WAIT** for about five minutes, or until the shell displays information. Your nvram values for the **date** in which you executed this command are now backed up in your **/opt/var/backups** directory on your external hard drive. To restore them, after upgrading your firmware/changing routers and **enabling usb access** in services/usb, navigate to the /opt/var/backups folder. Type "ls" to see the backups and then execute the **dated script** with the **essential.sh** tag. Type "./{backupfilename.sh}" to restore that backup. Sit back, let it do it's thing, and enjoy not having to manually reset nvram settings!

NOTE To Automatically have your router backup you configuration you can use CRON.

Navigate to Administration and make sure CRON is enabled. In the CRON box, add the following, then hit Save and then Apply.

```
4 4 * * * root /opt/usr/sbin/backupessential
```

Now your router will automatically backup your nvram setting every night. This more convenient than doing it manually.

For further discussion on this see this page: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=44324

Transmission

- **Transmission** - "Service Transmission Start" starts this and it can be accessed at 192.168.1.1:9091. However it will write to the /mnt/Torrent/work directory it defaults to using **non-root** permissions. the Group that is writes to is **www-data**. You now should make sure the directory exists. Verify that is accessible either by Samba or WinSCP. To access the torrents, you must enable samba on the router (easiest) or you can use WinSCP from a windows machine.

Relocate Syslog

- '*Reloc_Syslog* ***- A very valuable service that relocates the default syslog from /tmp/var/log/messages to /opt/var/log/messages. This is very beneficial as it does not use*** **any** of the router RAM to store **Optware** log messages, effectively reducing CPU/RAM resources, and will survive reboots enabling you to review your logs after rebooting. The entire tutorial is based around this service, so it is vital that you enable it and use it!

```
service reloc_syslog on
service reloc_syslog start
reboot
```

Make sure it works:

```
tail -f /opt/var/log/messages
```

if not using the reloc_syslog service

```
tail -f /var/log/messages
```

AsiaBlock

- **Asiablock** - This service is perhaps the single most valuable tool for your network. Whether you are just a normal user, or you are running an FTP/Web-server, this will add vital security to your data and peripheral devices.

By default it is not enabled. To enable it, open up either a telnet/SSH prompt, login, and enter **service asiablock on** followed by **service asiablock start.**

Once the start command is issued, you will see the service scanning IP range subnets from various countries around the world that are a potential threat to your network security. Once they are downloaded, you will now have enhanced security that is configurable to your specific demands.

Countries that are blocked by default are:

1. cn = China
2. af = Afghanistan
3. au = Australia
4. pk = Pakistan
5. in = India
6. my = Malaysia
7. ua = Ukrain
8. ng = Nigeria
9. kh = Cambodia
10. li = Liechtenstein

You can also add or remove countries by editing the Asiablock Script using VIM. To do this, shutdown Asiablock with the **stop** and **off** parameters, then type **vi /opt/etc/init.d/S95asiablock**

It is wise to know what you are doing before you do this though. Search the forums or the net for instructions.

To further enhance this service, you will need to add the following to your rc_firewall in Administration->Commands:

NOTE For users with PPPoE connections, use the command **wanf=`get_wanface`** for the WAN interface wildcard variable.

```
wanf=`get_wanface`
iptables -I INPUT 2 -i $wanf -p tcp -j asia
iptables -I FORWARD 1 -i $wanf -p tcp --dport 20:1024 -j asia
```

This happens to be my personal firewall that provides excellent security from Asian and other hackers/bots.

The dport 20:1024 -j asia rule prevents IP subnets dictated by asiablock from performing a portscan in order to hack either my FTP, SSH, Telnet, SNMP etc.

Here is a logged event of just such an attempt (notice the **DROP** and the attempted port **22**):

```
Apr 15 12:28:52 Asus user.warn kernel: [asia DROP] : IN=vlan2 OUT=  MAC=00:0c:41:bd:f3:0c:00:01:5
root@Asus:~#
```

Firewall and Iptables command scripts/tutorials can be obtained in many locations, including this sites Forum and Wiki.

Another useful trick included into Asiablock is the spam-list and ham-list (or approved IP subnets). For instance, if you wanted to "add" a IP subnet to Asiablock for blcking purposes (could be an angry co-worker or friend) use the following command (The **94.76.128.0/18** is the CIDR IP subnet range you want to block.):

```
echo 94.76.128.0/18>>/opt/etc/asia.spam
```

That IP is just an example, but you can obtain your specified IP subnet you want to block by using the **whois** command for the IP that is a potential threat (the 0.0.0.0 shall be replaced by the IP):

```
whois 0.0.0.0
```

To ensure that it took effect, first type **service asiablock start** (restarts the firewall) then issue the following command which will list all Asiablock IP bans:

```
cat /opt/var/log/messages | grep asia | grep -o "SRC=.* DST" | sort -u
```

Another useful command that will display your firewall integrity is:

```
iptables -nvL | more
```

Hit enter to continue with the readout

As the Asiablock script is still in the experimental stage and subject to change due to either build bug fixes or for enhanced usability, it is wise to update it periodically. (once every 2 weeks should suffice)

To do this, simply insert the following into a shell prompt and type **service asiablock start**)

```
wget -O /opt/etc/init.d/S95asiablock http://wd.mirmana.com/S95asiablock_2010
service asiablock on
service asiablock start
```

Update If you are tired of the [Asia DROP] messages filling up your router's logs, it is now possible to limit them using the newly created reloc-syslog service (explained above). To do this you must do the following:

- Enable and start the reloc_syslog service
- Download the latest version of Asiablock service:

```
wget -O /opt/etc/init.d/S95asiablock http://wd.mirmana.com/S95asiablock_2010
service asiablock on
```

- Edit the S95asiablock script using Vi. Find the variable *LOGONCE=0* and change it to **1**.

```
# Make sure Optware programs come first as they support a
export PATH=/opt/usr/sbin:/opt/sbin:/opt/bin:/bin:/usr/bi

# Constants

# cn = China
# af = Afghanistan
# au = Australia
# pk = pakistan
# ph = philippines
# in = india
# my = malaysia
# ua = ukrain
# ng = nigeria
# kh = cambodia
# li = Liechtenstein
# These countries will be blocked specifically
ISO_spam="af cn in pk my kh li vn kr ph"
ISO_ham="us"

# You can limit the amount of logentries per minute
LOGONCE=1

KEYWORD=asia
NAME=asiablock

URLBASE="http://www.ipdeny.com/ipblocks/data/countries"
AGE=10

CONFDIR=/tmp/etc/config
```

- Now hit esc and type :wq (write and quit).
- Reboot the router.

- After rebooting (give ~1 minute to settle) restart your terminal session. Issue the following command to see the process at work.

```
grep asia /opt/var/log/messages | grep -o 'SRC=[0-9.]* ' | sort | uniq -c | sort -n
```

For more information or questions, visit this thread:

http://www.dd-wrt.com/phpBB2/viewtopic.php?t=61346&postdays=0&postorder=asc&start=0

StopHammer

- **Stophammer** - A very unique and ingenious script written by frater. The service essentially monitors /var/log/messages for ANY evidence of a brute-force/DoS attack/etc. It works as a cron-job that monitors syslogd (must be enabled to work!) every 15 minutes for any signs of a malicious user or users attempting to probe open ports on your network. Once the user(s) are detected, it appends the IP(s) to a custom iptables chain called "syn-flood". Once the flood is detected, the service outputs the iptables chain to a file located in */opt/etc/iptables.hammer.rules* , which can also be customized.

To enable the service, and make sure it is working, do the following:

```
service stophammer on
service stophammer start
```

To make sure it is working, open up a shell prompt and enter the following:

```
tail -f /opt/var/log/messages
```

Now go to a portscanning site (my personal favorite is ShieldsUp!) and watch what happens ;)

https://www.grc.com/x/ne.dll?bh0bkyd2

Fixtables

- **Fixtables** , another Great feature is this service . This service fixes vital security flaws (and overall improper default configuration) by creating additional iptable rulesets. It can also act as a way of Preventing_Brute_Force_Attacks using the netfilter projects 'recent' matcher. It turns out that *-m limit x/min* is an improper way of enforcing this type of security.

It also adds the INVALID state, which inspects packets before they reach the WAN and automatically determines if they are, well, VALID! This will improve your network "cleanliness" quite a bit.

A few processes that the script handles are as follows:

1. Moves traffic coming from lan to lan to top of FORWARD chain
2. Removes lan2wan rule and only moves it back if it is in use with Access Restrictions
3. Moves traffic coming from br0 to almost top of the INPUT chain
4. Moves the RIP drop coming from LAN above the ACCEPT on the INPUT chain
5. Moves traffic coming from local to almost top of the INPUT chain
6. Creates an **INVALID** entry right after **ESTABLISHED** on the INPUT chain
7. Creates a **ratelimiter** for PING (ICMP) on the INPUT chain from the WAN
8. Moves Forwards to Lan IP from FORWARD to INPUT

9. Sets a MaxLoginRate limit for Proftpd to 1/min
10. Applies the **[BRUTEPROTECT]** mechanism even if your build does not have the recent module.
11. Fixes the current **loopback** issue in current builds that is creating many problems for some...

The service is already enabled by default, but may require a start:

```
service fixtables on
service fixtables start
```

Pixelserv

- **Pixelserv** , A very valuable service that increases web browsing security at the routing level (no host-based services that actually create more Adware than they block). When enabled (alongside the **xinetd** service), the script modifies several nvram variables and downloads a blacklist of malicious Ad Host DNS names. The nvram variables that are changed are *Use Local DNS* , adds **addn-hosts=/opt/etc/pixelserv/blacks** to DNSMasq options, and creates a false bridge interface that points to a bogus 10.63.63.1 IP that serves a 1x1 .gif image. It also moves DD-WRTs Web-GUI port to 88 instead of 80. Essentially this service performs **DNS Cache Poisoning**, but in a more "elegant" way ;)

Networked Printing

- **Networked Printing** - A very convenient service for allowing users on your network to print to a dedicated print server. To get this to work, make sure you have the **LATEST** build!

After plugging your USB printer in, open up a Telnet/SSH prompt and type **service xinetd on** followed by **service xinetd start** . After that type **service watchprinter start** . Wait about 5 minutes and then setup your printer in Printers and Faxes. This procedure is documented both Here and the net.

Accessing services in web browser

You can also turn a service on or off through the web interface command line in **Administration-> Commands** (for people who don't like the hassle of SSH):

Examples:

```
/opt/usr/sbin/service transmission-daemon on
/opt/usr/sbin/service transmission-daemon start

/opt/usr/sbin/service xinetd on
/opt/usr/sbin/service xinetd start
```

Choose the service(s) you wish to execute and click **Run Commands** in the Administration->Commands box.

You are ready to go! **It is also wise to wait at least 30 seconds after enabling these services before accessing them.**

Some services have their own web interface:

- **Swat/Samba - http://your.routers.ip:901**
- **Torrent Transmission - http://your.routers.ip:9091**
- **Twonky Media - http://your.routers.ip:9000**

If you would like to install **rtorrent** with **rutorrent**, have a look at this article Rtorrent_rutorrent_lighttpd

SD/MMC Method

- Made possible by DHC_DarkShadow

After and including build 13309

1. Make sure you have 13309 or higher on your router. Start with a fresh system 30/30/30 reset.
2. Partition the card - partition1 data, partition2 opt, partition3 jffs,partition4 swap reference How to - Format and Partition External Storage Device.
3. Boot router.
    1. Enable SD support. The firmware will automount the first partition to /mmc.
    2. Enable jffs.
    3. Setup your internet connection.
    4. Save the following script to **Startup** in **Administration->Commands.**
        1. mount /dev/mmc/disc0/part2 /opt (Note: if you formated like described http://www.dd-wrt.comhttp://www.dd-wrt.com/wiki/index.php/How_to_-_Format_and_Partiti use command: mount /dev/mmc/disc0/part3 /opt)
    5. automount will do the rest
4. Log into the router via Putty (SSH) and run fraters script below. This will take a while. It will tell you when it's finished.
    1. wget -O /tmp/prep_optware http://wd.mirmana.com/prep_optware
    2. sh /tmp/prep_optware
5. When the script is done, it will tell you so and advise a reboot. (it is wise to wait ~1-2 mins after completion before rebooting)
6. Reboot

Before build 13309

First off credit goes to frater for the optware script and the driver script credit goes to aszu and the startup script for the driver goes to phuzi0n. My hats off to you guys.

An update on my situation. The SD cards speeds were too slow and were overwhelming the router. I have steps for anyone using SD. It uses the new driver for the install. I have tested this 4 times on 2 different sd cards.

Start with a fresh system 30/30/30 reset, a **Clean** formatted SD card in either ext2 or ext3 with a /jffs directory, then create /opt inside of /jffs. Ex. /jffs/opt.

For some reason the later builds have a problem with formatting a card on setup, it screws the partition making the card invisible to the router. The above remedies this, and a service ticket has been submitted to fix this.

Continuing:

1.

- Boot router.
- Enable and setup GPIO's in the GUI for the SD Mod, because in the later builds auto GPIO is broken. Also setup your internet connection.
- **Enable jffs.**
- Copy the SDHC driver from HERE to the root directory of the MMC card via WinSCP
- Save the following script to **Startup** in **Administration->Commands.** This Startup script will run the new SDHC driver all the time. It is only necessary until the release of a build with it all ready ported.

Code:

```
cp /mmc/sdhc-gpio2.o /tmp
umount /mmc
rmmod mmc
insmod /tmp/sdhc-gpio2.o
mount /dev/mmc/part1 /mmc/
mount --bind /mmc/jffs /jffs
mount -o bind /mmc/jffs/opt /opt
```

2. Log into the router via Putty (SSH) and run fraters script below. This will take a while. It will tell you when it's finished.

Code:

```
wget -O /tmp/prep_optware http://wd.mirmana.com/prep_optware
sh /tmp/prep_optware
```

3. Reboot (it is wise to wait ~1-2 mins after completion before rebooting)

Notes

Useful scripts

```
mount - Shows what disks/partitions are mounted
fdisk -l - Shows disk information
blkid - Shows disk information
df -h - Shows disk usage and available space.  Very important
lsusb - Shows devices in /dev/usb/ like printers, USB hubs etc.
top - Shows all running processes and resources as well as swap file usage and CPU-Memory usage.
htop - A more user friendly application that allows you to kill processes, change their "nice" va
```

```
netstat -lnp - Shows which ports are open and what services are using them.
cat /tmp/fdisk
cat /tmp/blkid
cat /opt/etc/automount
cat /opt/etc/nomount

cat /var/log/messages - Shows the kernel logs if Syslogd is enabled.  Useful for debugging or vie
cat /opt/var/log/messages - Shows the Optware logs.  Great for information.
```

- You may find it easier to browse the logs using parameters separated with a **|** such as **more** and **grep** . **Grep** means find, and **more** will allow you to view the entire log one line at a time by pressing or holding down **Enter** . The parameters can also be used in conjunction:

Example :

```
root@Asus:~# cat /var/log/messages | grep Linux
Jan  1 00:00:06 Asus user.notice kernel: Linux version 2.6.24.111 (root@dd-wrt)
(gcc version 4.1.2) #1058 Wed Mar 24 04:18:19 CET 2010
root@Asus:~#
```

cat /var/log/messages | grep Linux | more

- To remove this optware completely (which should be done after a build upgrade, or if you don't need all of these services) do the following:

```
cd /opt
rm -r *
```

- When using USB storage (or maybe other form of storage as well), in order to automount the remaining partitions, the packages 'util-linux-ng' and 'grep' should be installed as well:

```
ipkg-opt install util-linux-ng
ipkg-opt install grep
```

Many more exciting packages are in the works, so be sure to follow This forum thread and further help is always available on the forums.

Enjoy!

Kernel 2.6 Problems! [READ!]

Currently (As of Build 13972), Media Servers (Twonky, Mediatomb, UShare, Etc) are not working under the 2.6 Kernel! If you want to use these services, use the 2.4 Kernel!

There are several commands to get the kernel build version: cat /proc/version

NOTE: I just installed dd-wrt mega, and it is build 14594 as of 2010-07-29. I will return to verify if this is still the case after installing.