This guide appears to be obsolete:

- The discussion thread no longer exists on FON's boards, and a search for "DD-WRT" or username "AustinTX" turns up nothing.
- The URLs to the heartbeat software no longer work.

Apologies to anyone requesting keys off me; I've been really busy, lacking a suitable working device to do it with, and not had time to fix one. Please add comments to this thread on the FON boards for complaints, insults and updates :o) UPDATE: AustinTX on the boards should be getting keys to anyone who's PM'd me for them over the last, err... 3 months? Yes I suck.

Welcome to the DD-WRT Fon Hotspot setup guide. If you have tried previous DD-WRT FON setup guides without success then fear not; the following guide has been tried and tested on three seperate routers with identicle success on each. It should be simple enough for anyone to walk through the guide so you don't need to know anything about coding or command line editing.

At the end of the guide you should end up with a registered FON hostpot using two wireless SSIDs, one private encrypted network and a seperate open FON hotspot network, and the original FON heartbeat function is included to show your hotspot as active on maps.fon.com. FON's online router personalization setup will still work, though any changes to the free website, router name, friends & family and wi-fi bandwith share settings won't work via the website although you can still change all of these (other than f&f) in the following setup guide.

Lastest Updates:

20/02/09 - Changed cron jobs to use spaces instead of tabs to avoid text corruption.
19/06/08 - Updated requirements section and other minor changes for v24 final firmware.
03/06/08 - Altered echo part of chillispot and startup script to correctly add new line if needed.
24/05/08 - Notes added on blocked MACs and correct registration routine. Please add to working mac list if you succeed.
17/05/08 - Changed Without JFFS Support to use wget file downloads.

29/01/08 - Added Registration errors section.

Contents

References

The information used in the guide was compiled from various sources along with including original info. If you want to know more about the setup, or have a problem with some specific parts, the next few links may help you out.

http://www.geek-pages.com/articles/latest/dd-wrt_-_multiple_ssids_-_1_for_fon_-_1_for_private_network.html

http://startu.net/chilli/setup.html

http://fon.freddy.eu.org/heartbeat/

http://boards.fon.com/viewtopic.php?t=1838&postdays=0&postorder=asc&start=20

FON On DD-WRT w/ Chillispot

Known Bugs

1. A bug in the latest releases (inc. RC1 to RC3) causes both the wland and chilli daemons/services to continually increase memory usage until no memory is left, causing a reboot after ~3 days on systems with 16 MB RAM. This bug is currently being worked on (see http://svn.dd-wrt.com:8000/dd-wrt/ticket/192) so should be fixed in a later firmware release, but for now you should implement the Memory Leak Workaround details in the guide. **This bug is fixed in v24-preSP2 and the workaround is no longer needed with current versions of DD-WRT.**

2. The only other small bug is chillispot not starting properly if it is first executed without an internet connection to the router. Precausions have been taken to avoid this in the code; see the troubleshooting section for more info. **As of v24-preSP2, ChilliSpot can be configured via the Web GUI and managed via DD-WRT's inbuilt process manager; it seems to be started in the correct order.**

Requirements

Router: WRT54G, WRT54GL, WRT54GS, or any DD-WRT router capable of running Chillispot. This guide may not work on the actual La Fonera router, but see FON_Hotspot_on_La_Fonera for one that does.

MAC: If you want to use your router as an official fon hotspot, and see it activated on maps, you need to use a FON compatible MAC address (see Registration).

The guide has been tested on a WRT54GL 1.0, 1.1 and WRT54G 2.0.

Firmware: DD-WRT v24 RC1 or RC3 NoKaid (dd-wrt.v24_generic_nokaid.bin v24 RC1 (08/22/07) or RC3).

Other versions allowing dual SSID and chillispot support should work depending on bugs, and versions without JJFS2 space (eg. Standard) can also be used but see Without JFFS at the end of the guide for slight changes in setup. RC1 and RC3 NoKaid are the only versions fully tested and supported in the following guide.

DD-WRT v24 Final will *only* work on a WRT54G(L) when following the Without JFFS section as neither Std or NoKaid versions feature free JFFS anymore, and no other versions with free JFFS feature chillispot support. I've asked in the forums for a custom build to be made featuring both chillispot and free jffs space but don't hold your breath, unless you fancy compiling one yourself?

FON: Registered user with pre-registered router or router's unique key.

You must be a registered FON user to setup a FON Hotspot. Non-registered routers can be registered using the following guide, though see the Registering New Routers section for more.

Registering New Routers

The FON Hotspot created during this guide will only work if the router has already been registered with FON. This can be done either by registering the router while it is running the official FON firmware, or by having access to a seperate FON router for which you have SSH access. Pre-registered routers need no further input, but for non-registered routers you need to access a uniquely generated key to register the router.

If you do not have access to either of these, send a PM to pepsi_max2k or AustinTX on boards.fon.com or contact me (pepsi_max2k) any other way, provide your WLAN MAC address and I will generate the key for you.

Blocked MACs

Also note that FON will block the registration of various MAC addresses. A selection of these are below and can be used as a guide, but I've done no extensive testing. Thing is, these MAC addresses have nothing to do with your router and are just referenced by FON from three variables in two code scripts. So err... technically, you could use whatever you like. I'd suggest using a fonera's mac (any of the 3), but obviously not to piss about just making things up as most MACs rightly belong elsewhere.

Working: 00-18-84, 00-18-39, 00-12-17.
Blocked: 00:1D:7E, 00-90-D0.

I guess you can assume most 00-18's work. Logging in to a fon hotspot on a blocked MAC address will actually just behave like a normally registered router. If you're still an alien you'll be redirected to a charge page, otherwise you'll get you're user page and be allowed normal web access.

Official Firmware

The official firmware is available at www.fon.com/en/download for the Linksys WRT54G, GL, GS v1-4, Buffalo WZR-RS-G54, WHR-G54S and HP-G54. If you have one of these routers you may want to get the unique key by just connecting to the router's FON Hotspot and accessing the FON login page. At this point, copy everything in the URL up until the variables starting ?res= and jump to the router setup part of this guide.

Manual Key Generation

Otherwise you must generate the key manually using a seperate FON router. The main aim is to generate a unique key from FON based on your router's MAC address. On official FON routers this is done by running the following code on bootup, where xx-xx-xx-xx-xx-xx is the wlan mac address of your router in **lower case** letters, separated by **dashes** (if you're unsure of yours, check the Status > Sys-Info page on your intended DD-WRT FON router for the **Wireless MAC** address).

You need to log in to your official FON router with SSH or telnet (see stefans.datenbruch.de/lafonera/#kolofonium for details on how, and use putty for SSH) and copy / paste the following code (replacing xx-xx... with your intended DD-WRT FON router's **WLAN** mac address in **lower case** letters):

```
/usr/sbin/chilli_radconfig -c /dev/null --radiusserver1=radius01.fon.com --radiussecret=garrafon
```

As soon as you press enter, around 20 lines of code will be printed out, ending in something that looks like the following:

```
uamserver https://www.fon.com/login/gateway/sec/9c3370131faaxxxxxxxxxxxxxxxxxxx
net 192.168.182.0/24
dynip 192.168.182.0/24
dns1 208.67.222.222
dns2 208.67.220.220
```

The thing you're looking for is the line starting "uamserver https://www.fon.com/login/gateway/sec/...". The long random looking 32 digit string after /sec/ is the key needed to register your router for the first time (I've added x's to the end of mine above to avoid you copying it ;o). Make a note of this **exact** key (copy and paste if you can) as you'll need it to register your router for the first time.

if you want to use your dd-wrt router download the executable to your router and then run it

```
wget http://trac.freewlan.info/browser/trunk/usr/sbin/chilli_radconfig?format=raw -O /tmp/chilli_
chmod +x /tmp/chilli_radconfig
/tmp/chilli_radconfig -c /dev/null --radiusserver1=radius01.fon.com --radiussecret=garrafon --adm
```

Heartbeat

One important part of registration is the heartbeat. This needs to be run before you try and register (see heartbeat section for howto). If you don't run it and connect to a non registered router you will see the AP_DOES_NOT_EXIST error in the URL for a sec after you've logged in, and then be redirected to a charge page. Just run the heartbeat a couple times in a row and it'll dissapear.

Registration Errors

If you have problems registering the router when you log on the first time (like never seeing a registration form), check the various redirect URLs that pop up in the address bar when you log in. You'll probably have to Ctrl-C them quickly then paste them somewhere as they only appear for a second or less. Any registration errors will appear in capital letters, with the first two stopping you from registering any new routers:

USER_IN_BLACKLIST

You are put in a blacklist whenever 100% of your previously registered FON routers have had their heartbeats off for around 3 days. Therefore, if you have no FON routers registered previously, you shouldn't get this error. If you do, you'll have to run the heartbeat for at least one of your routers for around three days until you are un-blacklisted.

AP_DOES_NOT_EXIST

This error pops up when no heartbeat has ever been run before trying to register. Run it and it'll go away.

NOT_ENOUGH_CREDIT

Can be confusing if you see it; it actually can come up regardless of whether you are a linus, bill or alien with or without credit. Usually it comes up just before you're redirected to a new router registration page, or before you're redirected to a charge page if you're either trying to register a blocked mac, or if you do indeed just not have enough credit.

Router Settings

The following should generally be followed in the order written so as to avoid any more reboots than needed or any complications with settings. Many settings are meant as a guide and can be changed to suit your own needs (IP, passwords, etc) but may cause unforseen problems as they're untested. Settings not mentioned can also be changed when needed (NAT, QoS, other services) but bear in mind that the router will not have much free memory left with the given settings so you may experience problems if you enable too many other services.

You should start with etiher a fresh install of v24 RC1, or **reset to defaults** using the reset button on the router.

Administration > Management

The first settings you should change are those in the Admin > Management tab, specifically the password and enabling JFFS2.

```
Router Password
Router Username: yourusername
Router Password: yourpassword          Change this to avoid unathorised access from hotspot users
Re-enter to confirm: yourpassword

Web Access
Protocol: HTTP
```

```
Auto-Refresh (in seconds): 3
Enable Info Site: Enable
Info Site Password Protection: Enabled  Tick to avoid hotspot users seeing the info site.
Info Site MAC Masking: Enable

Remote Access
Web GUI Management: Enable
Web GUI Port: 8080

Boot Wait
Boot Wait: Enable

Cron
Cron: Enable                            This MUST be enabled for the Hotspot to work.

Loopback
Loopback: Enable

802.1x
802.1x: Enable

Reset Button
Reset Button: Enable

Routing
Routing: Enable

JFFS2 Support
JFFS2: Enable
Clean JFFS2: Enable                     Enabled at this point incase JFFS space is not free.

Language Selection
Language: english

MMC/SD Card Support
MMC/SD Card Support: Disable

IP Filter Settings (adjust these for P2P)
Maximum Ports: 1024                     Max ports should be kept as low as possible to free memor
TCP Timeout (in seconds): 190
UDP Timeout (in seconds): 120

Overclocking
Frequency: 200 MHz

CIFS Automount
Common Internet File System: Disable
```

You should now click the **apply** button and then the **reboot router** button in order to clear the JFFS2 space properly.

Once rebooted, refresh this tab and check that the JFFS2 Total / Free Size contains a second value greater than 0, eg 384.00 KB / 60.00 KB. This confirms that 60 kilobytes of JFFS space has been freed. If this value reads 0, either try to clean the JFFS again or you may need to use a further stripped down version (you did use nokaid, right?), a router with greater RAM available, or check the section in this guide titled Without JFFS Support.

Setup > Basic Setup

Once the router has rebooted, browse to the Setup > Basic Setup tab and change the settings in order to get your internet connection active. Take note of your (automatic) MTU setting (specifically if using PPPOE) as if it differs from 1500 then you'll need to fix a bug with chillispot later on. The following settings assume a DHCP connection though you can change mostly everything to suit your needs.

WAN Connection Type
Connection Type: Automatic configuration : DHCP
STP: Disable

Optional Settings
Router Name: DD-WRT
Host Name:
Domain Name:
MTU: Auto 1500

Router IP
Local IP is 192.168.1.1.
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
Local DNS: 0.0.0.0

Network Address Server Settings (DHCP)
DHCP Type: DHCP Server
DHCP Server: Enable
Start IP Address: 192.168.1.100
Maximum DHCP Users: 20 *Kept as low as possible to free memory.*
Client Lease Time: 1440 Minutes
Static DNS 1: 208.67.222.222 *You can leave these blank to use your ISPs DNS,*
Static DNS 2: 208.67.220.220 *but I use OpenDNS.org's DNS servers.*
Static DNS 3: 0.0.0.0
WINS: 0.0.0.0
Use DNSMasq for DHCP: Ticked
Use DNSMasq for DNS: Ticked
DHCP-Authoritative: Ticked

Time Settings
NTP Client: Disable *Disabled to free memory, only enable if really needed*

Now press the **apply** button to save and enable these settings.

Setup > DDNS / Other

If you wish to setup a DDNS service then you should do so now (remember to click **apply** once you're done).

If you wish to change any other settings under the Setup tab you should also do this now, though I don't advise this as it may cause unforseen problems with the hotspot.

Wireless > Basic Setup

Due to problems running chillispot on the physical wireless interface, interfaces must be set up as follows with the private on physical and hotspot on virtual. You should also not alter anything other than the SSID names and wireless channel to suit your circumstances, with the SSID Broadcast setting being left enabled for at least the virtual (hotspot) interface and NoEncryption added to the hotspot name to assure people that it's not really encrypted incase they see it as such (we'll go over that later when we test).

First click the **Add button** under Virtual Interfaces to add one VI, then fill in the following details.

```
Physical Interface wl0
Wireless Mode: AP
Wireless Network Mode: Mixed                 Allows as many people as possible to connect to hots
Wireless Network Name (SSID): wrt54gl_wpa2   Change to suit your needs.
Wireless Channel: 1                          Change to suit your needs.
Wireless SSID Broadcast: Enable
Sensitivity Range: 2000
Network Configuration: Bridged

Virtual Interfaces wl0.1
Wireless Network Name (SSID): FON_FREE_INTERNET_NoEncryption      Recommended, but change to suit
Wireless SSID Broadcast: Enable              You want people to know it's there, don't you?
AP Isolation: Enable
Network Configuration: Unbridged
Multicast forwarding: Disabled
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
```

Now click the **apply** button to save and enable these settings.

Wireless > Wireless Security

Wireless encryption should be left disabled for the FON Hotspot for obvious reasons, and can be changed to whatever you like on the private WLAN though again for obvious reasons should not be left disabled otherwise people will just connect to that instead of the FON SSID for free net access.

```
Physical Interface wl0
Security Mode: WPA2 Personal Mixed
WPA Algorithms: TKIP+AES
WPA Share Key: xxxxxxxxxxxxx          I use a 13 digit key, change to whatever you like.
Key Renewal Interval: 3600

Virtual Interface wl0.1
Security Mode: Disabled               Don't be silly by enabling it :oP
```

Now click the **apply** button to save and enable these settings.

Wireless > Advanced Settings

If you wish to change any other settings under the Wireless tab you should also do this now, though I don't advise this as it may cause unforseen problems with the hotspot.

Administration > Commands (Firewall)

The following code is used to create a firewall on your router blocking access to the private network from the hotspot and how fast a connection hotspot users can get; a number of these rules can be added or changed. It also includes a **very important bug fix** for those of you with an MTU other than 1500 (mostly PPPOE users) so pay attention!

The main lines blocking access to the network are the *"iptables -t nat -I PREROUTING -i tun0 -d xxx.xxx.xxx.xxx/xx -j DROP"* lines. The first of these DROP lines **should be changed** to your router's own Local IP Address and Subnet Mask (see Setup > Basic Setup); the other DROP lines can be removed if you so wish but as they stand will block access to all privately used IP addresses. You **must keep** the *...192.168.182.1/32 -j ACCEPT* rule in to allow hotspot clients to access the Chillispot server.

The DOWNLINK and UPLINK values (in Kbps) limit the speed of any uploads or downloads by FON Hotspot users and can be changed as you see fit; currently they're set to 1 Mbps down and 256 Kbps up.

A bug in Chillispot causes connection problems to websites (specifically https and larger domains) while using a PPPOE connection from the DD-WRT router with an MTU other than the default Ethernet value of 1500. Therefore, if using such an MTU value, you **MUST** un-comment (remove the leading # from) the first iptables line in the firewall code to enable Chillispot to function correctly. This *does not* apply if you have a seperate modem that connects to the net using PPPOE but then connects to the rest of your network (eg. your dd-wrt router) using a regular local IP address / 1500 MTU.

NOTE: If your MTU is different from 1492 (PPPOE default), you must replace the 1452 in the line with your current MTU value minus 40. Eg, if your MTU is 1362, replace the 1452 in the code with 1322 (that's 1362 - 40).

```
#!/bin/sh

##

# IF USING MTU OTHER THAN 1500 (PPPOE), uncomment following line and change 1452 to your mtu minu
# iptables -t mangle -A POSTROUTING -p tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1452:65535 -j

iptables -I INPUT -i tun0 -j ACCEPT
iptables -I FORWARD -i tun0 -o vlan1 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i tun0 -o ppp0 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i br0 -o tun0 -j logdrop

# secure access to local addresses other than chillispot
iptables -A FORWARD -i tun0 -j DROP;

# change the following line's IP and Subnet to that of your routers (if not identicle)
iptables  -t nat -I PREROUTING -i tun0 -d 192.168.1.1/255.255.255.0

iptables  -t nat -I PREROUTING -i tun0 -d 192.168.0.0/16 -j DROP
```

```
iptables -t nat -I PREROUTING -i tun0 -d 169.254.0.0/16 -j DROP
iptables -t nat -I PREROUTING -i tun0 -d 172.16.0.0/12 -j DROP
iptables -t nat -I PREROUTING -i tun0 -d 10.0.0.0/8 -j DROP
iptables  -t nat -I PREROUTING -i tun0 -d 192.168.182.1/32 -j ACCEPT

DEV="tun0"
# change UP/DOWNLINK values (in kbps) to alter hotspot users up/download speeds
DOWNLINK="1024"
UPLINK="256"

tc qdisc del dev $DEV root
tc qdisc del dev $DEV ingress

# limit download
tc qdisc add dev $DEV root handle 1: htb
tc class add dev $DEV parent 1: classid 1:1 htb rate  ${DOWNLINK}kbit burst 6k
tc filter add dev $DEV parent 1: protocol ip prio 16 u32 match ip dst 192.168.182.1/24 flowid 1:1

# limit upload
tc qdisc add dev $DEV ingress handle ffff:
tc filter add dev $DEV parent ffff: protocol ip u32 match ip src 0.0.0.0/0 police rate ${UPLINK}k
```

Copy and paste the above code in to the commands box and click the **save firewall** button.

Connect To Internet

If it is not online already, ensure that your router has a working internet connection now as the following setup relies on one.

If the router connects directly to the internet, browse to the Status > Router tab and click the Connect button, otherwise ensure your LAN has an internet connection active. You should be able to open a web browser on a PC connected to the router and browse the net, and ping web addresses from the router's telnet prompt (*ping www.google.com*).

Telnet

You should now log in via telnet (or SSH if required) to run the various commands that will enable the hotspot, and check that everything is running smoothly.

Start by opening a command prompt in Windows (Start > Run > type cmd then hit OK) or Linux (you may need to install telnet). Type "telnet 192.168.1.1" minus the quotes, where 192.168.1.1 is your router's IP address if not ...1.1. You should now be asked for a login name; regardless of what you've set in the router this will be "root" without the quotes. The password will be the same as you've set on your router, in my guide this is "yourpassword".

When I ask you to enter code below, enter it line by line and hit enter at the end of each line to run the command before moving to the next line. You can paste copied lines in to telnet by a simple right mouse button click.

Check JFFS Space

Type the following to ensure that your JFFS space has been cleared correctly. You should see a blue "tmp" listed if it has, otherwise you should ensure that you are using the NoKaid firmware version and have enabled JFFS2 and Clean JFFS2 in the Admin web tab then clicked the apply then reboot buttons.

```
cd /jffs
ls
```

Enable FON Heartbeat

All routers running official FON firmware send a "heartbeat" signal back to fon every few hours once they're connected to the internet, mainly to update the router's online status on maps.fon.com and let FON know you're part of their community. To do this, you need to implement the FON Heartbeat in DD-WRT by downloading the heartbeat code originally created by Freddy. You can read more about this code at http://fon.freddy.eu.org/heartbeat/ .

NOTE: The heartbeat uses port 1937 to send information so ensure that this port is not blocked by a firewall on your router. If you're unsure, it's probably open anyway.

Ensure Cron is enabled on the Admin > Management web page and then type (or paste) the following into the telnet prompt to download the files.

```
cd /jffs
wget http://fon.freddy.eu.org/heartbeat/fonkey
wget http://www.inaudible.co.uk/perm/nolog/thinclient
chmod 755 /jffs/thinclient
ls
```

After the ls, ensure that you see both the fonkey and thinclient files listed, the latter being a light green colour.

Now start the heartbeat script by typing the following code into telnet:

```
/jffs/thinclient start
```

After a minute or two wait, the following line should be printed out, but with your own Wireless and LAN MAC addresses listed.

```
sent: mode='start' wlmac='00:18:39:xx:xx:xx' mac='00:18:39:XX:XX:XX' fonrev='3' firmware='0.6.6'
Something is wrong, /tmp/.thinclient.sh is empty
```

Ignore the final warning; the heartbeat should now be up and running and appear active on maps.fon.com. If not, check the troubleshooting section below for more help.

Chillispot

The most important part of the whole hotspot; Chillispot controls the FON hotspot functionality including login details and "free" website access. After creating the chilli.conf file, a number of things are customizable including DNS addresses and additional uamallowed lines or addresses, though keep in mind that much of the information is critical to the currect functioning or the hotspot.

We start by downloading the chilli.conf file to /jffs and adding your WLAN MAC address to it (in capitals separated by commas, it'll add a line like "radiusnasid XX-XX-XX-XX-XX-XX").

Type the following in to telnet:

```
cd /jffs
wget http://www.inaudible.co.uk/perm/fon/chilli.conf
echo -en "\nradiusnasid `nvram get wl0_hwaddr|sed -e s/:/-/g`\n" >>/jffs/chilli.conf
```

If you already have a registered router and don't want to add your own "free" websites or change DNS servers then you can just skip this next edit part and jump to Enable Chillispot.

Edit Chilli.conf

If you have not already registered your router with FON, you'll need to know your router's unique key as detailed in the Registering New Routers section of this guide and edit the chilli.conf file with vi. You'll need to add /sec/ and your unique key to the end of the uamserver line using the vi editor. Do this by typing in:

```
vi /jffs/chilli.conf
```

You can now hit "i" to enter text insert mode, use mouse cursors to move to the end of the uamserver line and edit it so that it looks like the following (ensure the 9c... bit is actually your 32 digit unique key, and no trailing / at the end).

```
uamserver https://www.fon.com/login/gateway/sec/9c3370131f....
```

If you wish to **change the dns** server addresses you can (the backspace or delete key should help), though I use OpenDNS.org's servers. If you wish to **add your own website** to the "freely" accessible ones for hotspot users, add them to the end of the last uamallowed line **without the http://** but with a , at the beginning so that it looks a little like so:

```
uamallowed labs.fon.com,213.134.44.0/23,www.fonshop.com.tw,shop.hk.fon.com,maps.naver.com,www.myw
```

Once you have done editing the file, you should exit the edit mode by hitting the Esc key, enter command mode by hitting the : key (shift plus ;) and then save it by typing wq!. In other words, type the following:

```
:wq!
```

If you mess anything up, you can quite without saving by just typing !q and start again.

Now type "more /jffs/chilli.conf" and check that the chilli.conf file is identicle to the above code (bar edits) and contains the correct radiusnasid line at the end (including your WLAN MAC in capitals separated by commas, v. important). If so, we shall continue. Otherwise you can delete the chilli.conf file by typing "rm

/jffs/chilli.conf" (careful, rm is powerful) and start again.

Enable Chillispot

You can now start chillispot by typing the following command in telnet:

```
/usr/sbin/chilli --conf /jffs/chilli.conf
```

You shouldn't see any errors, but if you do it's probably because you typed out the chilli.conf file wrong. Just go back to the above and start again. Now type the following:

```
top
```

and, assuming your router is connected to the internet, you should see a chilli and possibly thinclient service running, chilli taking up ungodly amounts of memory. If so, all is well and you can exit top by hitting Ctrl-C, and exit telnet by typing "exit" (or just close the command window).

Memory Leak Workaround

Due to a memory leak in certain DD-WRT releases (inc. RC1 to RC3) affecting the chilli and wland services, you may need to implement the following fix to restart both chilli and wland periodically. **This bug is fixed in v24 pre SP2 and the workaround is no longer needed in current releases of DD-WRT.**

The fix involves creating two extra files in the /jffs folder. Both can be edited with vi if needed, details of usage can be found in the Create Chillispot Config File section though it basically involves hitting **i** to enter text and **esc** then type **:wq!** to write and quit.

You also need to run these files using cron, and an extra two lines have been added to the startup command script (just bellow) to allow this. Note that although both scripts are set to run at midnight (when people are least likely to be connected), **if you have the ntp service disabled** (recommended) then you should **follow the Set Date & Time section below**, otherwise midnight will be determined as the point you first boot the router.

Killwland

The first file is used to kill the wland daemon. So far no one's actually figured out what this does, and wireless usage is seemingly unaffected by killing it outright, but to be on the safe side we'll just restart it once a day.

You just need to download the file **killwland** to /jffs and make it executable with the following code:

```
cd /jffs
wget http://www.inaudible.co.uk/perm/fon/killwland
chmod 755 /jffs/killwland
```

Killchilli

The second file is used to kill the chillispot daemon and runs once every 2 days. Basically it checks to see if there's anyone connected to the hotspot (set up on wl0.1 as per above guide, change this if needed) and if not, restarts chilli. If someone is connected, it will wait 8 minutes and try again. It will do this three times and if not successful on the third try, will give up and try again in another 2 days. If you run a heavily used hotspot this may cause problems, so you can edit the file with vi to either increase the sleep (wait) time, or change the KILLEND value to try more times before giving up.

```
cd /jffs
wget http://www.inaudible.co.uk/perm/fon/killchilli
chmod 755 /jffs/killchilli
```

Set Date & Time

If you have the ntp daemon disabled then the router will not know the correct time when it is booted, and will default to Jan 1st 1970 with a time of 00:00 once it's booted. This is fine unless you want to run watchdog scripts or make sure the above killstuff scripts actually run at midnight. In this case, you can set the time on the router by using the following command, where 010215352007 is the Month (01), Day (02), 24hr Time (1535) and Year (2007) respectively so change to suit.

```
date -s 010215352007
```

It will then print out the date and time, in this case showing Tue Jan 2 15:35:00 UTC 2007. You can use either the *date* or *uptime* commands to show you the current date and/or time in the future. Unfortunately there's no real way of doing this automatically (if the router don't know the time, it don't know the time...) so you'll have to do this again if you ever reboot the router without the ntp daemon started.

Test Wireless Connections / Register Router

You can now test out your new Wi-Fi private and hotspot networks, but you should bear in mind that differing makes of wi-fi recievers will see the encryption and broadcast settings differently regardless of setitngs. In my experience, the hotspot will at times be recognized as encrypted (when it's not) and you may never see the private physical SSID in a wireless network search, so you may need to provide correct details manually when connecting to either SSID.

So, start with the private interface and as I say you may have to enter details manually into your laptop / PC's wifi settings. You should recieve an IP in the range of your router's Local IP and have full access to the net. If so, on to the hotspot...

Again, if you're seeing the hotspot as encrypted, you may need to manually change the encryption to none and open to connect properly. Once you do, you should gain an IP address in the 192.168.182.X range so long as chillispot is running. Once you do, open a browser and you should be redirected to the FON login page when you try to access any page other than those in the "free" uamallowed lines in chilli.conf. Once you login, **if this is an unregistered router and you added your unique key correctly** you will be asked to register this router to your account. Otherwise you will just see the normal FON user page and now have full access to the web.

If anything goes wrong with the FON Hotspot connection, go through the above guide again paying attention specifically to the FON virtual interface settings, MTU/PPPOE bugfix in the firewall code, chilli.conf setup and starting the chillispot service.

Administration > Management (Cron)

Once you're satisfied that your Hotspot is functioning correctly, you now need to add just a bit more code in the Web control panel to run the various scripts and programs setup above.

First you need to copy and paste the following code to the Additional Cron Jobs box in the Admin > Management tab. Note that you must use single spaces between the time commands, otherwise the web interface will mess it up and add special characters which'll stop the cron jobs from running.

```
24,54 * * * * root /jffs/thinclient cron > /dev/null 2>&1 &
0 0 * * * root /jffs/killwland > /dev/null 2>&1 &
1 0 */2 * * root /jffs/killchilli > /dev/null 2>&1 &
```

Now click the **Apply Settings** button.

Depending on the internal time (see Set Date & Time), the first line will run the heartbeat on the 24th and 54th minute of every hour, and the second and third are used for memory leak problems, restarting wland every day at midnight, and chilli every other day at 1 min past midnight.

Administration > Commands (Startup)

Now on the Admin > Commands tab, you need add the following code to your router's startup commands in order to start chillispot (the FON Hotspot) every time it is turned on / rebooted. You may wish to alter the sleep value (in seconds) if you think it'll take longer that 6 minutes for your router to establish a full internet connection. This is important as chillispot may not run correctly if it is started without an internet connection, although once running it will stop and start at will whenever the connection is dropped for a short time.

```
#!/bin/sh

# wait for net connection at boot (in secs, alter if it takes longer for you)
sleep 420

# kill chilli incase already started by cron job
/usr/bin/killall chilli
sleep 5

# start chilli
/usr/sbin/chilli --conf /jffs/chilli.conf
```

Copy the above code in to the commands box and click the **Save Startup** button.

Optional: Free More Memory

At this point you may be seeing a rather low amount of free memory on the status tab. This can cause unforseen problems, especially on routers with heavy traffic, such as reboots every 3 days or so. Because of this you will likely a) not want to use the hotspot on any critical routers and b) free up as much memory as possible in order to limit the amount of problems it could cause. Here's a few optional but recommended things you can do to achieve this:

Disable All Unneeded Services

Check the Services tab for any un-needed services. Other than DNSMasq and Telnet (esp if disabling HTTP below), you shouldn't need any of them. Also make sure things like NTP and DDNS are only enabled if needed.

Security > Firewall / VPN

Go to Security > Firewall and **tick Filter Multicast**. This will stop the igmprt service from running, but will also stop any multicast packet transmission which may affect some online videos. Hit **Apply** to save.

On the Security > VPN tab, **disable all passthroughs** (IPSec Passthrough, PPTP Passthrough, L2TP Passthrough). Unless you use VPN these shouldn't be needed and will free up some memory. Hit **Apply** once more to save.

Lower User Connections

You can also lower the number of connections by users, both DHCP clients and port / tcp usage, to avoid the router being taken down by excessive connections. The choice is down to you, but...

Setup > Basic Setup, under DHCP **lower Maximum DHCP Users** to as low as you feel you can get away with. Remember you need at least your own private PC / PCs and hotspot users connected but anything between 10 and 20 should be more than enough for most.

Administration > Mangement, under IP Filter Settings you could **change Maximum Ports to 1024** or even 512, though serious P2P users may not want to. TCP Timeout can also be lowered to 120 if you don't foresee problems doing so. Once done, hit **Apply** to save the settings.

Disable HTTP Control Panel

Although handy, the web based control panel takes up more memory than any other process bar chillispot, so going without is the best way to free some up. If you do, you should **ensure telnet is enabled** as this is the only control you'll have left unless you do a full reset. Even though, I **recommend doing this**.

Ensure Services > Services **telnet is Enabled** then go to the Administration > Mangement tab and under Web Access **untick HTTP and HTTPS** and also **disable the Enable Info Site option**. Now click **Apply** settings and **Reboot Router**.

That's it, you're now command line only. Telnet into the router and type/enter **top** or **free** to see how much memory you've freed up. Other useful commands are **uptime** which'll hopefully last longer now, **wl assoclist** to show wireless clients, **more /tmp/dnsmasq.leases** to show DHCP clients, and **/tmp/ppp/redial 01** to connect a PPPOE connection if it doesn't come up by default. **ifconfig** will show you a list of interfaces, including a ppp0 one with internet IP address once a PPPOE connection is up. **httpd** will temporarily enable the web control panel again and **killall httpd** will kill it once you're done, though you can enable permanently from within the control panel from the same tab you disabled it.

Final Reboot

Now click the **Reboot Router** button (under the Administration tab among others). If all goes well the router will restart and automatically run the heartbeat and chillispot once an internet connection is established. Watch the Memory section on the Status tab, specifically the Free and Buffers section for a significant drop once chillispot kicks in (usually around 7 mins after boot depending on startup sleep value). They should drop to between 300 and 800 kB, quite low which is why you should have disabled as many unneeded services as possible.

You should also be able to connect to both the private and hotspot networks as normal, and continue to do so unless the JFFS2 space is disabled (removing the heartbeat and chillispot files) which should only happen if you upgrade the firmware (in which case all settings will likely be reset anyway).

Also, if the internet connection is ever dropped by the router, chillispot will automatically stop until the connection is regained, at which point it will start right back up again on it's own.

Now, if you had problems or want to do stuff differently, read on. Otherwise, Happy Hotspot running!

Post-setup Changes

The FON website contains a Configure Your Router page where you can change details for official routers. Because we've set this one up manually, most of the stuff on that page won't work but here's how you can change the options on the router yourself.

For most changes you may need to enable the web control panel again if you have it turned off, so log in to telnet and type "*httpd*". To turn off the web control panel again, type "*killall httpd*".

Router Name / Password

The virtual SSID (FON_WIFI_HOTSPOT...) is the equivalent of FON's online "Router name" setting. It will not be changed if you alter it online, but instead you can change it on the Wireless > Basic Setup page whenever needed, although I don't recommened removing the first FON_ part as it may confuse people.

The password refers to both the wireless encryption and router login password. You can change both on the Wireless > Security and Administration > Management tabs.

How Much Wifi To Share

As with the name and password, changin the "How much Wi-Fi do you want to share?" option (which changes the download speeds) will have no affect. Instead, you can browse to the Administration > Commands tab, click Edit under the Firewall code, and change the UPLINK and DOWNLINK values (in Kbps) to change both the download *and upload* speeds. Then hit **apply** and the settings should apply immediately.

Friends and Family

Again, this won't do anything if you fill it in. I don't actually know how to accomplish this on the router, it's probably just another line in the chilli.conf file, but it doesn't matter anyway because all your friends and family can just log on to the private network anyway so the F&F option is redundant.

Edit: As of v24-preSP2, there is an option to add local ChilliSpot users via the DD-WRT GUI; note that you seem to need to add all your users at once and then Apply Settings directly (not Save first) owing to a bug in the GUI that will otherwise save your password as "blahblahblah". This has the effect of dumping username/password pairs into /tmp/fonusers.local and ChilliSpot then accepts these as local users via the FON login page. So, it works, but the GUI is broken.

You can work around that in nvram; these preferences are saved in the variable fon_userlist as a space-separated list of username=password pairs. In your startup scripts, feel free to add something like:

```
nvram set fon_userlist="keith=somepass michael=anotherpass"
```

before the nvram commit statement; this should set up your FON local users when the system boots and before ChilliSpot starts.

Other Online Changes

All other settings and charts on the FON website should function as normal, including the "Personalize your FON Spot" page, "My Router Log" and "Fon Passes" as these don't rely on sending information back to, and changing settings on, the router.

Other Router Setup Changes

You can also change most other settings on the router without causing any problems. Just remember that you want as much free memory as possible so enabling too much may cause crashes. Also, you shouldn't change the FON IP, or the subnet unless you change your router's main subnet. And if you do change the router's main IP or Subnet you'll probably have to change a few things in the firewall code too.

Chilli.conf / Telnet Changes

If you want to alter the options in chilli.conf you can do so in telnet using vi. When you're done, type "*killall chilli*" then start chilli again with the usual "*/usr/sbin/chilli --conf /jffs/chilli.conf*" line or just reboot. Other changes to scripts in telnet will usually require the same coresponding kill process / restart process code. Use "*top*" to check what's running and what's not.

Differing Firmware Tips

Without JFFS Support

If for some reason you cannot enable JFFS Support then you can still setup chillispot and the heartbeat, you'll just have you add some startup code to create the files at each boot. The chilli code can be altered in the same way as the chilli.conf file in the main guide. The heartbeat files are downloaded from my personal webserver as they have been slightly modified for temorary storage usage (/jffs changed to /tmp).

On the Admin > Commands tab, copy and paste the following in to the Commands box and then click the **Save Startup** button. Make sure you've also added the cron jobs as detailed above, with the change in locations to ensure the heartbeat and memory leak files run correctly.

```
#!/bin/sh

# wait until net connection established
sleep 600

# get heartbeat files
cd /tmp
wget http://www.inaudible.co.uk/perm/thinclient
wget http://www.inaudible.co.uk/perm/fonkey
chmod 755 /tmp/thinclient

# create mem leak fix files
cd /tmp
wget http://www.inaudible.co.uk/perm/fon/killwland
wget http://www.inaudible.co.uk/perm/fon/tmp/killchilli
chmod 755 /tmp/killwland
chmod 755 /tmp/killchilli

# create chilli.conf
cd /tmp
wget http://www.inaudible.co.uk/perm/fon/chilli.conf
echo -en "\nradiusnasid `nvram get wl0_hwaddr|sed -e s/:/-/g`\n" >>/tmp/chilli.conf

# start chillispot
/usr/sbin/chilli --conf /tmp/chilli.conf
```

The script will now run at on every boot of the router so reboot now to start the heartbeat / chilli. The script will execute 10 minutes after booting (or running commands) to insure that an internet connection is active (mainly for PPPOE users).

With Log Support

If you're a sucker for logs and have them enabled on the router (which I don't recommend due to memory usage), you may want to use the heartbeat code with logging enabled. In which case, just use Freddy's original script and start it (in telnet or Admin > Commands > Startup) using the following code:

```
cd /jffs
wget http://fon.freddy.eu.org/heartbeat/fonkey
wget http://fon.freddy.eu.org/heartbeat/thinclient
chmod 755 /jffs/thinclient

/jffs/thinclient start 2>&1 | logger
```

Chillispot On Physical Interface

Due to a bug in RC1 stopping chillispot working with the physical wireless interface, chillispot cannot be setup from the web control panel as you cannot change the interface used from here (and it defaults to the physical one). If using an earlier firmware version such as 06/20 or SP1 and later then you can set up the FON hotspot / disable encryption on the physical interface and the private network / encryption on the virtual interface, then use the control panel to set up chillispot. The following settings mostly mirror the chilli.conf file above and you can personalise it in the same way. Note that the Radisu NAS ID must be your WLAN Mac address in upper case letters separated by dashes.

```
Sputnik: Disable
Wifidog: Disable

Chillispot: Enable
Seperate Wifi from LAN Bridge: Enable
Primary Radius Server: radius01.fon.com
Backup Radius Server: radius02.fon.com
DNS IP: 208.67.222.222
Remote Network: 192.168.182.0/24
Redirect URL: https://www.fon.com/login/gateway
Shared Key: garrafon
DHCP Interface: WLAN
Radius NAS ID: XX-XX-XX-XX-XX-XX
UAM Secret: garrafon
UAM Any DNS: 1
UAM Allowed: www.fon.com,www.paypal.com,www.paypalobjects.com,www.skype.com,www.google.com,www.fl
MACauth: Disable
Additional Chillispot Options: (copy and paste the following 6 lines into box)

uamallowed static.flickr.com,video.google.com,shop.fon.co.kr,secure.nuguya.com,inilite.inicis.com
uamallowed maps.fon.com,c20.statcounter.com,fon-en.custhelp.com,www.excite.co.jp,image.excite.co.
uamallowed 216.239.51.0/24,66.249.81.0/24,66.249.93.0/24,72.14.207.0/24,72.14.209.0/24,84.96.67.0
uamallowed 202.47.16.159,202.47.16.161,202.47.17.159,202.47.17.161,202.47.18.159,202.47.18.161,20
uamallowed ssl.google-analytics.com,c26.statcounter.com,www.fonshop.jp
dns2 208.67.220.220

HTTP Redirect: Disable
NoCatSplash: Disable
SMTP Redirect: Disable
```

Make sure that if you use this option, remove the lines running and/or downloading modifying the chillispot settings and daemon.

Troubleshooting

Troubleshooting Chillispot

1. Is chillispot starting with a network connection established? If the router does not have internet access when chillispot starts, it will not run correctly and remain so until a reboot. Either browse to the online Status pages and hit connect as soon as you've rebooted, or alter the sleep time in the startup script from 600 to something larger (remember, it's in seconds; 600 = 10 mins).

2. Do you get a 192.168.182.X addess when connected to the FON SSID? If not, chillispot isn't running correctly. Make sure the startup command and chilli.conf file are correct.

3. Do you have problems accessing any sites after connecting to the FON SSID, even with correct IP addess? If so you may have hit the MTU bug. See the Firewall setup section for a diagnosis / fix.

4. When you run */usr/sbin/chilli --conf /tmp/chilli.conf* you get the following printout: *Could not resolve ip adress of uamserver*. This is due to the router not being able to access the internet, in which case you should find that you can't access any websites either. Just ensure that your router has an internet connection before running this line (check the Status > Router tab and click Connect under the Internet section if needed). If you can access https://www.fon.com/login/gateway from a PC connected to the router you should be OK, otherwise check that the uamserver address in chilli.conf is identicle to the previous one, with or without /sec/youruniquekey... added.

Troubleshooting Heartbeat

The main clue to problems with the heartbeat is obviously the router spot on fon maps not going a dark green colour. Here's some things to check:

1. Are you connected to the internet / have you rebooted the router and gone through installing the heartbeat again? Obvious ones, but a simple problem to solve.

2. Has the script downloaded correctly? It's currently hosted on my personal website, so that may have been inaccesible while your router tried downloading files. You can try telneting in to the router and running all the commands from the script following the "sleep" command (and ignoring # comment lines). If you type ls in the /tmp directory you should see both files listed, with thinclient in green text to signify it has been chmod'ed correctly. After hitting enter on the final command there should be a slight pause but nothing more exciting.

2. Has the known_hosts file been downloaded to /tmp/root/.ssh/ ? If not, thinclient could either not connect to the internet, of one of the commands was wrong. Try running just "/tmp/thinclient start" to see if there are any error messages. The most likely thing is that you have either not managed to download fonkey or thinclient to the right place, you have not chmod'ed thinclient correctly or you edited thinclient wrongly.

3. Is your WLAN MAC being selected correctly by thinclient? From your router's ssh or telnet command line, run both "nvram show | grep wl0_hwaddr" and "nvram show | grep il0macaddr". If the first comes back blank, and the second comes back with your WLAN MAC, you need to edit thinclient with vi again to remove the first part of line 26, that's *WLMAC="$(/usr/sbin/nvram get wl0_hwaddr)" # original:* , and leave just *WLMAC="$(nvram get il0macaddr)"*. Now thinclient should correctly gather your MAC address which may

help in showing it as active on fon maps.