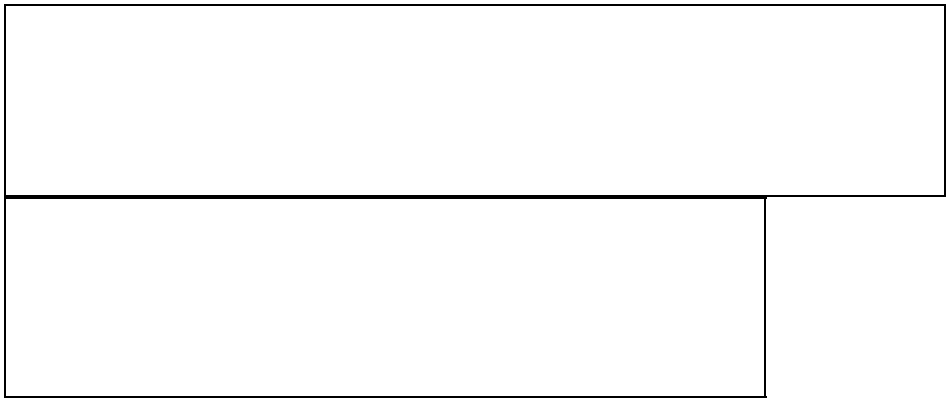
English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Option found in "Administration" > "HotSpot" > "HTTP Redirect"



This option enables an HTTP redirector for proxy usage. While it's located on the Hotspot configuration page, Hotspot does not have to be enabled for this option to work properly. The HTTP Redirector works by redirecting all port 80 traffic from the LAN/WLAN to a specified address which could be an HTTP proxy server like Squid, CCProxy, or Winproxy. This feature is especially useful for content filtering in schools, libraries, businesses etc.

It's not completely clear what the purpose of the "HTTP Source Network" setting is. In my tests, setting the IP address in here for only one of the client computers made no difference. All clients were proxied regardless. According to BrainSlayer "you can set a source network which excludes the proxy server", thereby allowing the proxy server to get it's Internet from the same router that has the HTTP Redirector enabled. So far, my tests of this feature, using a WRT54G with v23 SP2, have not produced good results.

HTTP Source Network

<The following tested in DD-WRT v24-sp2 (11/25/08) std - build 10991M NEWD Eko>

When using this feature you must specify the LAN side subnet that you want to be subject to the redirect. For example if you have DHCP set to dish your computers into 192.168.1.xx then enter 192.168.1.0 as your source network. It is not possible to redirect more than one source network to the proxy using this feature. Specifically if you enter 0.0.0.0 as your source network then DD-WRT writes bogus entries into the NAT table so that no traffic gets redirected.

DD-WRT actually creates two NAT table entries when this feature is enabled. The first entry makes sure that traffic from the source network destined for your router's web pages are not redirected but instead go directly to the router. The second entry redirects all other traffic to the proxy. The way this first entry is created makes it impossible to loose your connectivity to the router even if you make a mistake in entering data here.

You can use this feature to implement a HTTP-Proxy (like squid) connected on the LAN side of your router if you configure the proxy to have a different subnet than the rest of your computers. The idea would be for your proxy to be on its own special subnet (ie. 192.168.10.10) with all the other computers being in the standard subnet (ie. 192.168.1.xx). You would set the HTTP Destination IP to 192.168.10.10 and the HTTP Source Network to 192.168.1.0. DD-WRT would then only redirect port 80 traffic coming from your 192.168.1.0 subnet to your proxy. All other subnets would not be re-directed and the proxy server which needs direct

access the destination servers would be able to do its job.

This feature does a reasonable job of adding entries to the NAT table but unfortunatly never deletes them. This means that you can get horribly confused if you make a change to one of these settings and fail to reboot the router since you can have multiple and conflicting entries in your NAT table. So take my advice and do a "Save" followed by a reboot if you make any changes to the settings for HTTPRedirect.

Bad HTTP Redirector Settings

If you entered settings into your router's HTTP Redirector settings that were not correct, likely you are unable to log into the web interface because your request to the router's web server is being redirected to who-knows-where. You can use Telnet or SSH to fix this problem.

Telnet into the router.
Enter username and password.
Enter the following commands:

```
cd /usr/sbin
nvram set http_redirect_enable=0
nvram commit
reboot
```