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

OpenDNS is a free DNS (Domain Name Server) service which makes internet browsing safer and allegedly faster. By simply using their DNS servers instead of your ISP's you are automatically protected from their list of Phishing websites. However, in order to restrict a variety of adult website content you will need to create a free account with them, register your IP address and select the categories you want restricted (i.e. sexuality, nude, pornography, lingerie, grotesque, etc...). Since most of us have DHCP assigned WAN IP addresses that change periodically we need to instruct our router to tell OpenDNS what our new IP address is when it changes. We will go over that below.

Contents

- 1 Basic Setup
- 2 OpenDns with DNS-O-Matic for users with a Dynamic IP
- 3 Intercept DNS Port
- 4 Intercept DNS Port Specific Ip/Range
- 5 Performance Impact

Basic Setup

In order to configure dd-wrt with OpenDNS you need to specify the OpenDNS DNS servers in the control panel. This can be done in two ways: You can either configure your router to hand out the OpenDNS DNS addresses to your DHCP clients, or you can configure DNSMasq to forward all DNS requests sent to your router to OpenDNS. The advantage option 2 is that you will not lose internal DNS resolution on your network.

Option 1 - Configure DHCP with OpenDNS DNS servers

1. Go to **Setup** tab » **Basic Setup** sub tab » **WAN Setup** section » **WAN Connection Type**, and check "Ignore WAN DNS"
2. Go to **Setup** tab » **Basic Setup** sub tab » **Network Setup** section » **Network Address Server Settings (DHCP)**, and:
    - ♦ Set **Static DNS 1** to **208.67.222.222**
    - ♦ Set **Static DNS 2** to **208.67.220.220**
    - ♦ Depending on the behavior you want, set **Static DNS 3** set to:
        - ◊ **0.0.0.0** to fall back to your ISP DNS if OpenDNS is unresponsive; or
        - ◊ **10.0.0.0** (a non-usable IP) if you don't want to use any other servers; or
        - ◊ Another DNS server of your choice (Do not duplicate one of the first two DNS's or it will default to 0.0.0.0)
            - · **Note:** OpenDNS also has these DNS IP's that can be used for the 3rd Static DNS: **208.67.222.220** and **208.67.220.222**
            - · To ensure that all devices are restricted by OpenDNS Web Content Filtering you should configure all 3 Static DNS entries using the OpenDNS IP's.
    - ♦ Check the following options:

◊ Use DNSMasq for DNS
◊ DHCP-Authoritative
◊ Forced DNS Redirection

3. Click **Save**
4. Click **Apply Settings**

Tip: If you want the DNS servers to be queried in the order they're listed rather than randomly:

1. Go to **Services** tab » **Services** sub tab » **Services Management** section » **DNSMasq** sub section and ensure *Query DNS in Strict Order* is selected.
2. Click **Save**
3. Click **Apply Settings**

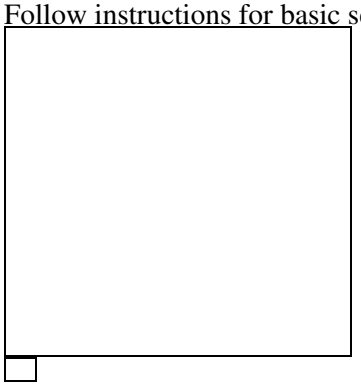
Option 2 - Configure DNSMasq for OpenDNS DNS forwarding

1. Go to **Setup** tab » **Basic Setup** sub tab » **WAN Setup** section » **WAN Connection Type**, and check "Ignore WAN DNS"
   - Click **Save**
   - Click **Apply Settings**
2. Go to **Services** tab » **Services** sub tab » **Services Management** section » **DNSMasq** sub section
   - Ensure **DNSMasq** is enabled
   - Ensure *Query DNS in Strict Order* is selected.
3. In the **Additional DNSMasq Options** text box, enter
   no-resolv
   server=208.67.222.222
   server=208.67.222.220
   - Click **Save**
   - Click **Apply Settings**

OpenDns with DNS-O-Matic for users with a Dynamic IP

OpenDNS provides an additional service for users with Dynamic DNSs. Their DNS-O-Matic will relay the request to OpenDNS and also optionally forward this to any number of additional Dynamic DNS providers.

1. Follow instructions for basic setup above.



DNS-O-Matic with dd-wrt

2. Setup an account with OpenDns and **Enable dynamic IP update** under the settings tab on the OpenDNS website. Also enable any filtering options you want.
3. Log into DNS-O-Matic. It shares the same username and password for OpenDNS.

4. Add OpenDNS as a service on DNS-O-Matic
5. Also add account information for any other Dynamic DNS providers you have.
6. Now click the "Update Info" radio buttion
7. On the **DDNS** tab under **Setup** in dd-wrt set **DDNS Service** to Custom.
8. Set **DYNDNS Server** to updates.dnsomatic.com
9. Fill in your Username and Password for OpenDNS/DNS-O-Matic
10. Set **Host Name** to all.dnsomatic.com
    - To update multiple hosts, use ***hostname1*** **-a** ***hostname2*** **-a** ***hostname3*** **-a** ***hostnameN*** Source: this tip.
11. Put /nic/update?hostname= in the **URL** text box.
    - If that doesn't work, use:

      ```
      http://updates.dnsomatic.com/nic/update?hostname=
      ```
    - If you get a badauth error from dnsomatic, it could be that you need to use https instead of http, so try:

      ```
      https://updates.dnsomatic.com:443/nic/update?hostname=
      ```
    - If you get a badauth error from dnsomatic, it could be that you need to use http instead of https but specify port 443, so try:

```
http://updates.dnsomatic.com:443/nic/update?hostname=
```

1. Apply

Intercept DNS Port

You can prevent users from using their own DNS servers (and hence get around content filtering) by intercepting DNS queries and forcing them to use the DNS servers you specify.

1. Go to **Administration** tab » **Commands** sub tab
2. In the **Commands** text box, enter:

```
iptables -t nat -A PREROUTING -i br0 -p udp --dport 53 -j DNAT --to $(nvram get lan_ipaddr)
iptables -t nat -A PREROUTING -i br0 -p tcp --dport 53 -j DNAT --to $(nvram get lan_ipaddr)
```

1. Click **Save Firewall** (note: your WAN interface will be restarted)

Intercept DNS Port Specific Ip/Range

Same as above but for a specific IP address/Range

1. Go to **Administration** tab » **Commands** sub tab
2. In the **Commands** text box, enter:

```
iptables -t nat -A PREROUTING -i br0 -s 192.168.1.128/25 -p udp --dport 53 -j DNAT --to $(nvram g
iptables -t nat -A PREROUTING -i br0 -s 192.168.1.128/25 -p tcp --dport 53 -j DNAT --to $(nvram g
```

Or

```
iptables -t nat -I PREROUTING -i br0 -s 192.168.1.128/25 -p udp --dport 53 -j DNAT --to 208.67.22
iptables -t nat -I PREROUTING -i br0 -s 192.168.1.128/25 -p tcp --dport 53 -j DNAT --to 208.67.22
```

1. Click **Save Firewall** (note: your WAN interface will be restarted)

Another way of intercepting DNS requests can be done in the "Access Restrictions" tab under "Blocked Services" and by choosing "dns" option in the list of services. Additionally, IP addresses and/or MAC addresses of the clients can be defined by clicking the "Edit List of Clients" button under "Access Policy".

Performance Impact

Do note that many major websites, download hosts and media sites are now using content delivery network. These network will resolve an IP that is closest to you for performance. Typically, when you use your ISP's DNS server, you will get an IP address within or close to your ISP's network.

If you choose to use OpenDNS, you will get IP addresses that are optimal to OpenDNS' network but maybe far away from your network. This will have performance impact for sites that are using content delivery networks.