# PG-13 Internet Safety Router Workshop
# April 19, 2015

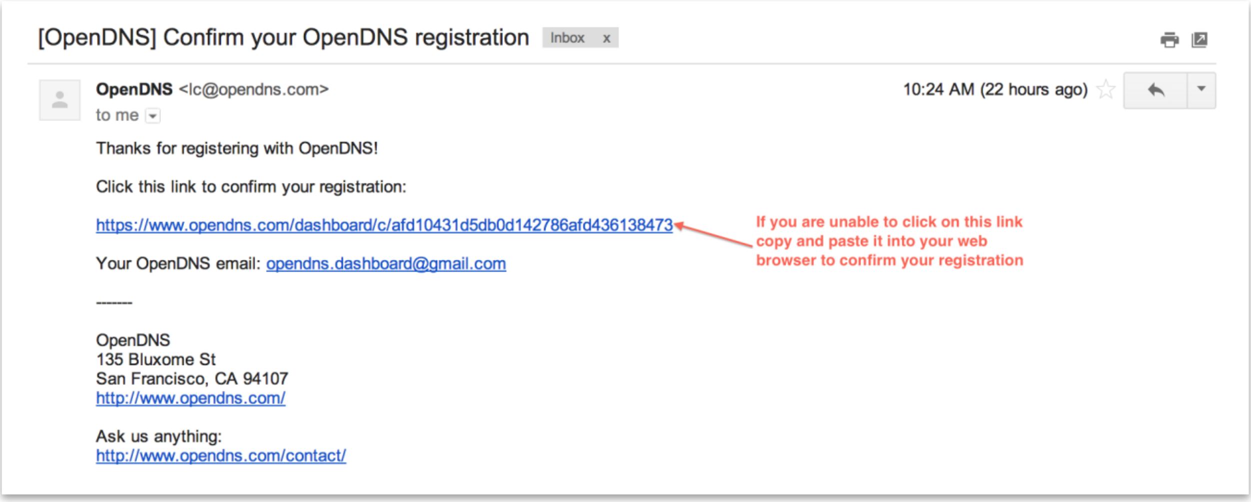
## Table of Contents

## Notes, Assumptions, & Prerequisites:

1. You have broadband internet. You want to protect your home. You recognize that the steps below will NOT protect you/your family against over-the-air data. Refer to the handout provided at the PG-13 event for more information. The steps below along with your new router protect your local wireless network only. **Connect the blue port on the router to port #1/WAN port on your modem.**
2. As you go through the following steps, please fill out of the "Checklist and Documentation". This is required in order to properly troubleshoot and keep you organized in the future when making changes.
3. When you see text in quotations (e.g. "password"), only use the text inside the quotes. Do not copy/paste the quotes. The quotes are there to make it clearer for you.
4. If you have Comcast, make sure you enable bridge mode if you have Comcast phone service; follow the instructions: http://customer.comcast.com/help-and-support/internet/wireless-gateway-enable-disable-bridge-mode/
5. If Comcast, make sure you disable Xfinity Hotspot; follow the instructions: http://customer.comcast.com/help-and-support/internet/disable-xfinity-wifi-home-hotspot/
6. (Ignore this step for the workshop; already done for you) You have a TP-LINK TL-WR841N v9 flashed to DD-WRT. If not, you can download the current latest build from http://download1.dd-wrt.com/dd-wrtv2/downloads/betas/2015/04-09-2015-r26653/tplink_tl-wr841ndv9/factory-to-ddwrt.bin. This assumes you get v9 which is the latest hardware. You can flash this version directly in the TP-LINK GUI.

## OpenDNS Setup *(OK to do away from home/ahead of time from Calvary Church)*

1. Go to OpenDNS and signup for a free account: https://www.opendns.com/home-internet-security/parental-controls/opendns-home/. Hit the "SIGN UP NOW" orange button. At right, enter your information to setup your account. **Write your username and password down on the checklist at the end; #1.**
2. Check your email for an account confirmation email from OpenDNS. Not all email services allow hyperlinks within the content of messages, if the link in your email is not clickable copy and paste the link into your browser to confirm your account. If you click (or copy and paste) the link in the confirmation email you will be taken to your OpenDNS dashboard.



[OpenDNS] Confirm your OpenDNS registration

**OpenDNS** <lc@opendns.com>
to me

10:24 AM (22 hours ago)

Thanks for registering with OpenDNS!

Click this link to confirm your registration:

https://www.opendns.com/dashboard/c/afd10431d5db0d142786afd436138473

If you are unable to click on this link copy and paste it into your web browser to confirm your registration

Your OpenDNS email: opendns.dashboard@gmail.com

-------

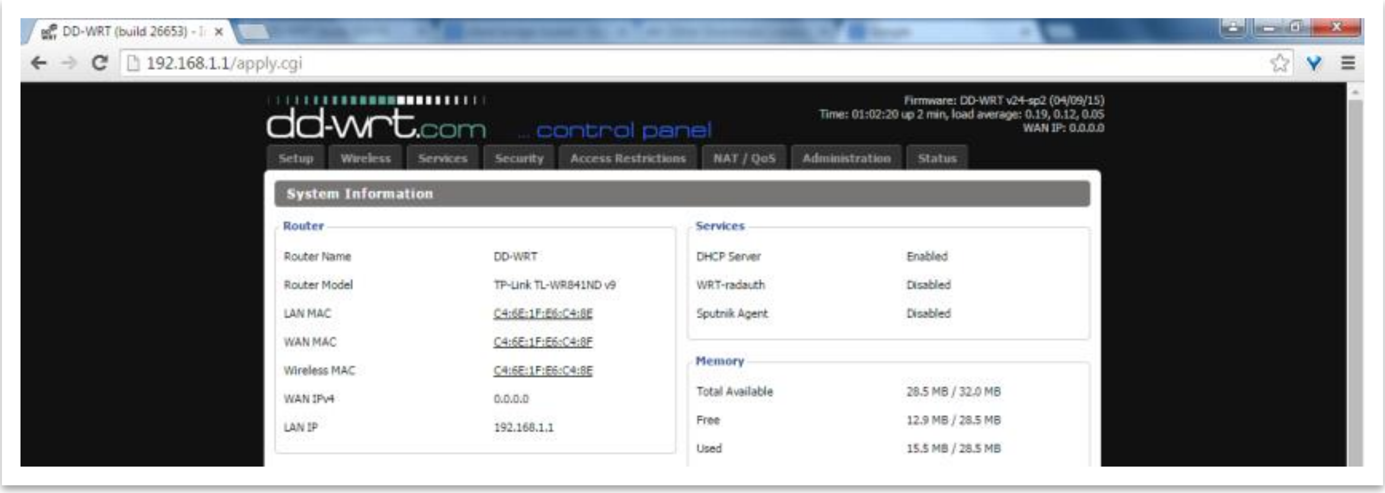
OpenDNS
135 Bluxome St
San Francisco, CA 94107
http://www.opendns.com/

Ask us anything:
http://www.opendns.com/contact/

3. Once confirmed, move on to router setup.

## DD-WRT TP-LINK TL-WR841N Router Setup

1. Go to http://192.168.1.1/



Firmware: DD-WRT v24-sp2 (04/09/15)
Time: 01:02:20 up 2 min, load average: 0.19, 0.12, 0.05
WAN IP: 0.0.0.0

System Information

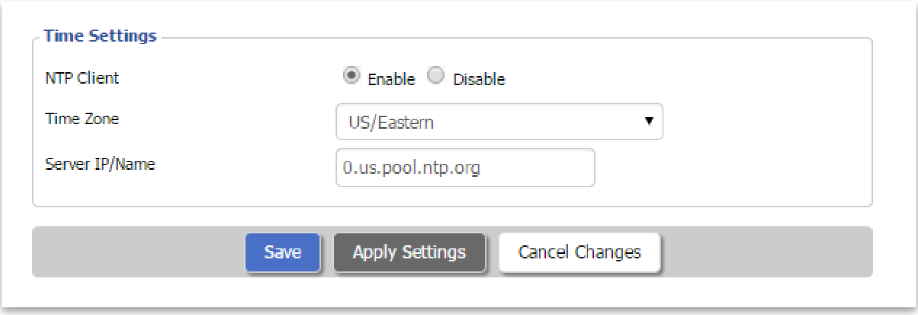
| Router | |
|---|---|
| Router Name | DD-WRT |
| Router Model | TP-Link TL-WR841ND v9 |
| LAN MAC | C4:6E:1F:E6:C4:8E |
| WAN MAC | C4:6E:1F:E6:C4:8F |
| Wireless MAC | C4:6E:1F:E6:C4:8E |
| WAN IPv4 | 0.0.0.0 |
| LAN IP | 192.168.1.1 |

| Services | |
|---|---|
| DHCP Server | Enabled |
| WRT-radauth | Disabled |
| Sputnik Agent | Disabled |

| Memory | |
|---|---|
| Total Available | 28.5 MB / 32.0 MB |
| Free | 12.9 MB / 28.5 MB |
| Used | 15.5 MB / 28.5 MB |

Click "Setup" at the top and enter the following when the webpage prompts you:
Username: "root" Password: "pg13"

2. First, change the default password of "pg13". At the top, go to "Administration". Scroll down and enter "root" as the username (overwriting the ••/***). Please enter a new password and re-confirm it; please make it something your kids cannot guess. **Write your username and password down on the checklist at the end; #2.** Scroll further down and check the box next to "Info Site Password Protection". Go to the bottom and hit "Save". This is the router password that you will need to make changes to the router in the future, and prevents your kids from changing settings.
3. Next, click on the upper left tab "Setup". It should take you to the "Basic Setup" sub-tab. Scroll down, feel free to name your router whatever you would like under "Router Name". Scroll to the bottom and enter the "Time Settings" as follows:



Time Settings

NTP Client: ● Enable ○ Disable

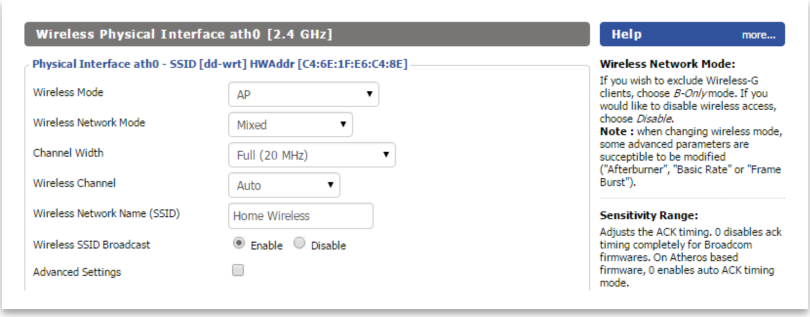
Time Zone: US/Eastern

Server IP/Name: 0.us.pool.ntp.org

Copy/paste to make data entry easier: 0.us.pool.ntp.org
Hit “Save”.

4. Click on the “DDNS” sub-tab at the top (next to “Basic Setup”). Select “Custom”. Enter the following information. Copy/paste below.
    a. DDNS Service: “Custom”
    b. DYNDNS Server: “updates.dnsomatic.com”
    c. <Enter your OpenDNS username and password you setup earlier; should be #1 on your checklist>
    d. Hostname: “all.dnsomatic.com”
    e. Under URL: “/nic/update?hostname=”

    Hit “Save” at the bottom.
5. Click on the “Wireless” tab at the top. Under “Wireless Network Name (SSID)” enter whatever you want the parents/adult/older kids network to be named. For demonstration, I am calling it “Home Wireless”. Hit Save.



Wireless Physical Interface ath0 [2.4 GHz]

Physical Interface ath0 - SSID [dd-wrt] HWAddr [C4:6E:1F:E6:C4:8E]

Wireless Mode: AP

Wireless Network Mode: Mixed

Channel Width: Full (20 MHz)

Wireless Channel: Auto

Wireless Network Name (SSID): Home Wireless

Wireless SSID Broadcast: ● Enable ○ Disable

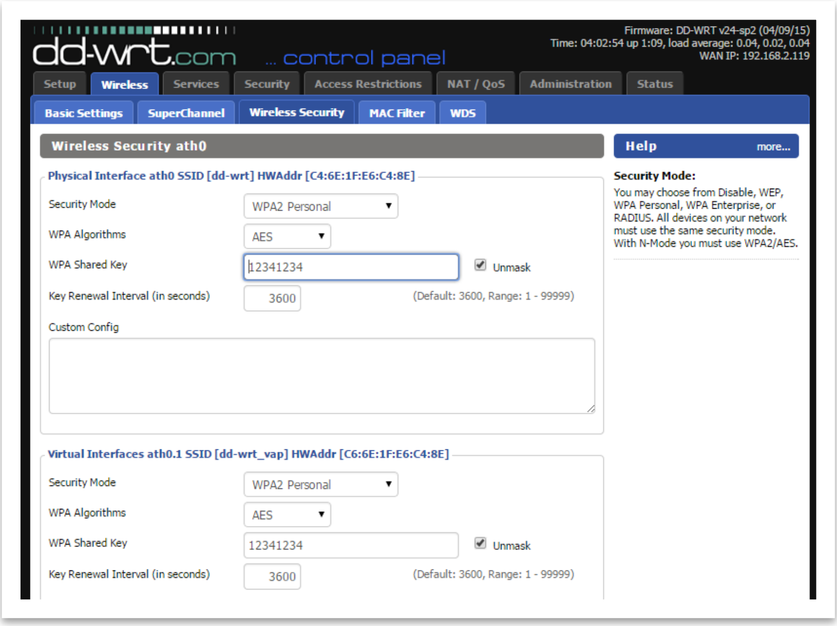
Advanced Settings: □

**Wireless Network Mode:**
If you wish to exclude Wireless-G clients, choose *B-Only* mode. If you would like to disable wireless access, choose *Disable*.
**Note :** when changing wireless mode, some advanced parameters are susceptible to be modified ("Afterburner", "Basic Rate" or "Frame Burst").

**Sensitivity Range:**
Adjusts the ACK timing. 0 disables ack timing completely for Broadcom firmwares. On Atheros based firmware, 0 enables auto ACK timing mode.

Once saved, click on “Add” under “Virtual Interfaces” and enter a network name “Wireless Network Name (SSID)” for the kids. For demonstration, I am calling it “Kids Wireless”. Hit Save.

6. At the top, go to “Wireless Security” and under “Security Mode” select “WPA2 Personal”. Under “WPA Shared Key” enter whatever password you want for your **parent** wireless network. In the example, this is the “Home Wireless” network. It must be 8 characters and should not be easily guessable and not shared with kids. Hit “Save”. **Write down the “Home Wireless” key on the checklist at the end; #3.**



Firmware: DD-WRT v24-sp2 (04/09/15)
Time: 04:02:54 up 1:09, load average: 0.04, 0.02, 0.04
WAN IP: 192.168.2.119

Wireless Security ath0

Physical Interface ath0 SSID [dd-wrt] HWAddr [C4:6E:1F:E6:C4:8E]

| | | |
|---|---|---|
| Security Mode | WPA2 Personal | |
| WPA Algorithms | AES | |
| WPA Shared Key | 12341234 | ☑ Unmask |
| Key Renewal Interval (in seconds) | 3600 | (Default: 3600, Range: 1 - 99999) |
| Custom Config | | |

Virtual Interfaces ath0.1 SSID [dd-wrt_vap] HWAddr [C6:6E:1F:E6:C4:8E]

| | | |
|---|---|---|
| Security Mode | WPA2 Personal | |
| WPA Algorithms | AES | |
| WPA Shared Key | 12341234 | ☑ Unmask |
| Key Renewal Interval (in seconds) | 3600 | (Default: 3600, Range: 1 - 99999) |

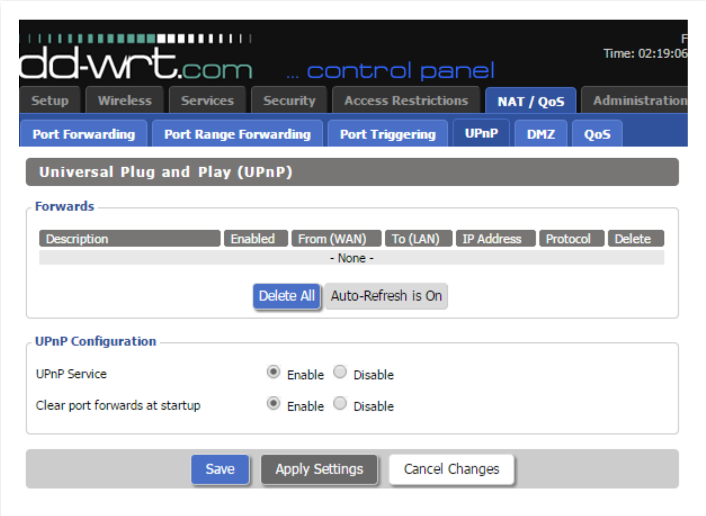
Security Mode:
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode. With N-Mode you must use WPA2/AES.

7. Do the same for the "**Virtual Interfaces ath0.1**"below. Make sure you hit "Save" from the step before then add the security information for the virtual interface. Select "WPA2 Personal", under "WPA Shared Key" enter whatever password you want for your **kids** wireless network. In the example, this is the "Kids Wireless" network. It must be 8 characters and given to your kids. **Write down the "Kids Wireless" key on the checklist at the end; #4.**
8. Next click on the "Services" tab at the top. Scroll down to the "DNSMasq" section. Under "Additional DNSMasq Options" copy/paste the following carefully.

```
no-resolv
server=199.85.126.20
server=199.85.127.20
address=/google.com/216.239.38.120
address=/google.ca/216.239.38.120
address=/www.google.com/216.239.38.120
address=/www.google.ca/216.239.38.120
```

After pasting, go to the bottom of the page and disable the last option: "ttraff Daemon". Hit "Save".

9. At the top, go to the "NAT /QoS" section. Then go to the "UPnP" submenu at top. Enable both the "UPnP Service" and "Clear port forwards at startup" options and hit save. See below.



Time: 02:19:06

Universal Plug and Play (UPnP)

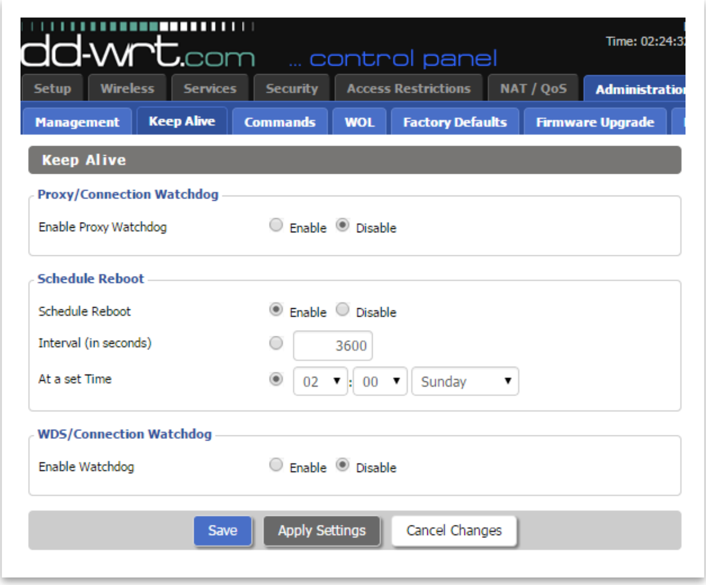
Forwards

| Description | Enabled | From (WAN) | To (LAN) | IP Address | Protocol | Delete |
|---|---|---|---|---|---|---|
| - None - | | | | | | |

UPnP Configuration

| | |
|---|---|
| UPnP Service | ● Enable ○ Disable |
| Clear port forwards at startup | ● Enable ○ Disable |

10. At the top, go to “Administration”.  Next, click on the “Keep Alive” sub-menu at top.  Hit enable for “Schedule Reboot”.  Enter when you want the router to automatically reboot itself to stay healthy.  I suggest 2:00am Sunday morning.  Select the radio button to the right of “At a set time” and choose “2” under the first drop-down menu.  Hit “Save”.



Keep Alive

Proxy/Connection Watchdog

Enable Proxy Watchdog ○ Enable ● Disable

Schedule Reboot

Schedule Reboot ● Enable ○ Disable

Interval (in seconds) ○ 3600

At a set Time ● 02 : 00 Sunday

WDS/Connection Watchdog

Enable Watchdog ○ Enable ● Disable

11. Go to the “Commands” sub-menu.  Copy/paste very carefully the following code into the “Commands” box.

```
#Append HomeWireless/non-marked traffic to local DNS server, NortonDNS, using the integrated DNSMASQ instance
iptables -t nat -I PREROUTING -i br0 -p udp --dport 53 -j DNAT --to $(nvram get lan_ipaddr)
iptables -t nat -I PREROUTING -i br0 -p tcp --dport 53 -j DNAT --to $(nvram get lan_ipaddr)

#KidsWireless DNS repeater instead of directly forwarding to OpenDNS to handle Google SafeSearch
sleep 5
dnsmasq -S 208.67.220.123 -S 208.67.222.123 -R -i br0 -p 54 --address=/google.com/216.239.38.120 --address=/google.ca/216.239.38.120 --
address=/www.google.com/216.239.38.120 --address=/www.google.ca/216.239.38.120

#Mark packets coming out of ath0.1 (KidsWireless)
insmod ebtables
insmod ebtable_filter
insmod ebt_mark.ko
sleep 2
ebtables -I INPUT -i ath0.1 -j mark --set-mark 2

#Append traffic for KidsWireless to local DNS server, OpenDNS, running on the manual instance of DNSMASQ on port 54
iptables -t nat -I PREROUTING -i br0 -p tcp --dport 53 -m mark --mark 2 -j DNAT --to $(nvram get lan_ipaddr):54
iptables -t nat -I PREROUTING -i br0 -p udp --dport 53 -m mark --mark 2 -j DNAT --to $(nvram get lan_ipaddr):54

#CRON key for setting up wireless timing
#minute (0-59),
#|        hour (0-23),
#|        |        day of the month (1-31),
#|        |        |        month of the year (1-12),
#|        |        |        |        day of the week (0-6 with 0=Sunday).
#|        |        |        |        |        commands
#
#For example to disable wireless between 9pm-6am (and disables it every hour the hour in between).  To override/extend access another hour just reset the router.
#0 21-23,0-5 * * * root ifconfig ath0.1 down
#0 6 * * * root ifconfig ath0.1 up
#
#Now how about turning off wireless only on S,M,T,W,TH nights? (O=Sunday)
#0 21-23 * * 0-4 root ifconfig ath0.1 down
#0 0-5 * * 1-5 root ifconfig ath0.1 down
#0 6 * * 1-5 root ifconfig ath0.1 up
#
```

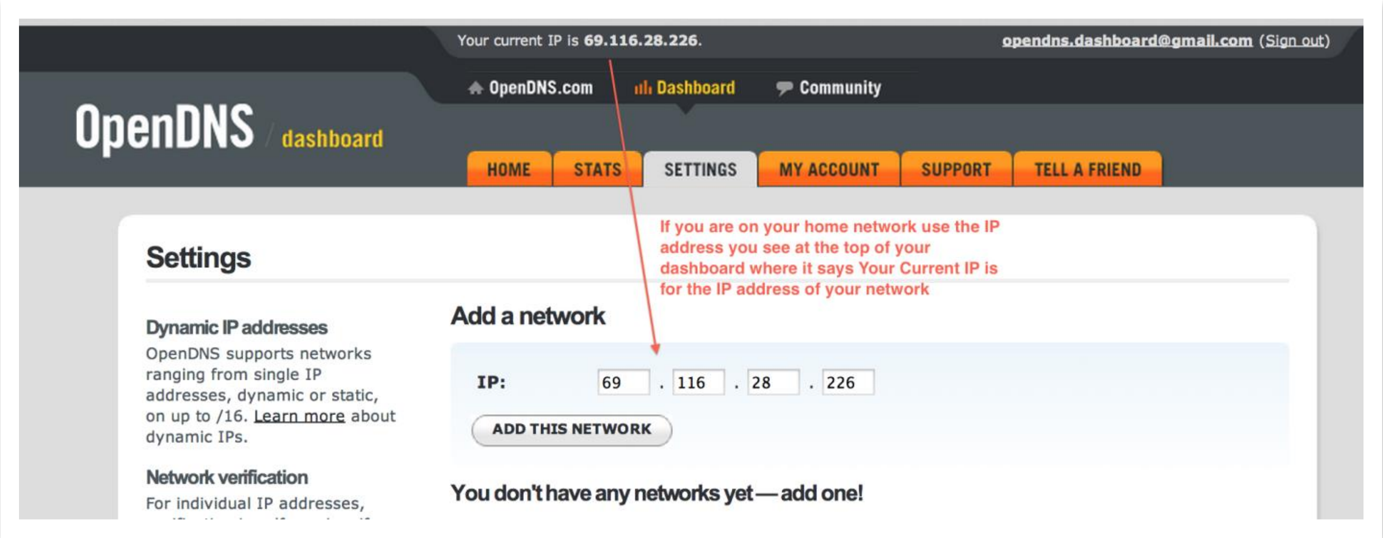
After pasting the code above, hit “Save Firewall”.  It will take roughly 30 seconds for the firewall script to save.

12. Lastly, go back to the “Management” sub-tab at the top, scroll the entire way to the bottom, and click the red “Reboot Router” button.

## Linking OpenDNS to your home internet ***(Do NOT do this away from home; do immediately when you get home!)***

1. First, go re-read section #1, “Notes, Assumptions, & Prerequisites” and ensure you have your Comcast or internet connection setup correctly.  Confirm you modem/internet connection is in bridge mode.  Your best option is to purchase your own modem (Motorola SB6141 is recommended) that does bridging by default.
    a. **The key is getting a public IP address assigned directly to your router.**  Not only will it make filtering work correctly, it will make the internet faster and allow ports to automatically be opened for certain devices (e.g. AppleTV, Roku, Chromecast, etc.) making those devices work better.
    b. To check if your router is getting a proper public IP address, login to http://192.168.1.1 and look at the upper right.  You will see a “WAN Address” line in white text.  If that number does NOT start with “10.x.x.x” or “172.x.x.x” or “192.x.x.x” (where “x” represents any number) you are good to go.  If that line starts with a 10, 172, or 192, then your modem is also a router and not in bridge mode correctly.  Please call your internet provider and have them walk you through getting the modem into bridge mode.

2. Login to OpenDNS. www.opendns.com. At the top, click on "Dashboard"
   (The steps and screenshots are from https://support.opendns.com/entries/53936430-Configuring-OpenDNS-on-your-Network with edits for working with DD-WRT.)
3. Next you need to "Add a Network". You will see a big box on your Home screen that says Add a network as shown below. Adding a network to your OpenDNS dashboard allows you to use our custom content filtering and stats features. Click on the Add a network box to get started:
   Once you click **Add a network** you will get the below screen which asks you to add an IP address. If you are on your home network you will see your current IP address displayed at the top of your dashboard where it says **Your current IP is**. Copy this number from the top of the screen. This is your current external (public) IP address that is assigned to you by your internet service provider as your network. Use that IP address for your dashboard network:



Your current IP is 69.116.28.226.

opendns.dashboard@gmail.com (Sign out)

Settings

If you are on your home network use the IP address you see at the top of your dashboard where it says Your Current IP is for the IP address of your network

Dynamic IP addresses

OpenDNS supports networks ranging from single IP addresses, dynamic or static, on up to /16. Learn more about dynamic IPs.

Network verification

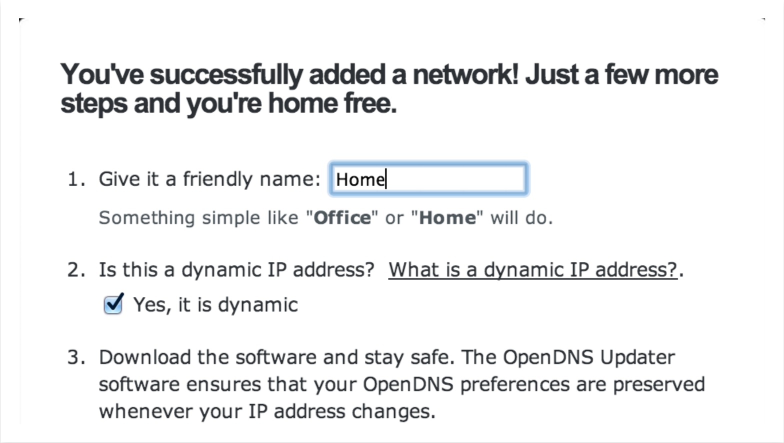
For individual IP addresses,

Add a network

IP: 69 . 116 . 28 . 226

You don't have any networks yet—add one!

4. Next you will get a screen that asks you for a network name and whether or not you have a **Dynamic** IP address. If you are unsure, you most likely have a dynamic IP address. Most internet service providers lease dynamic IP addresses which means that your IP address can change. Check off "Yes, it is dynamic".

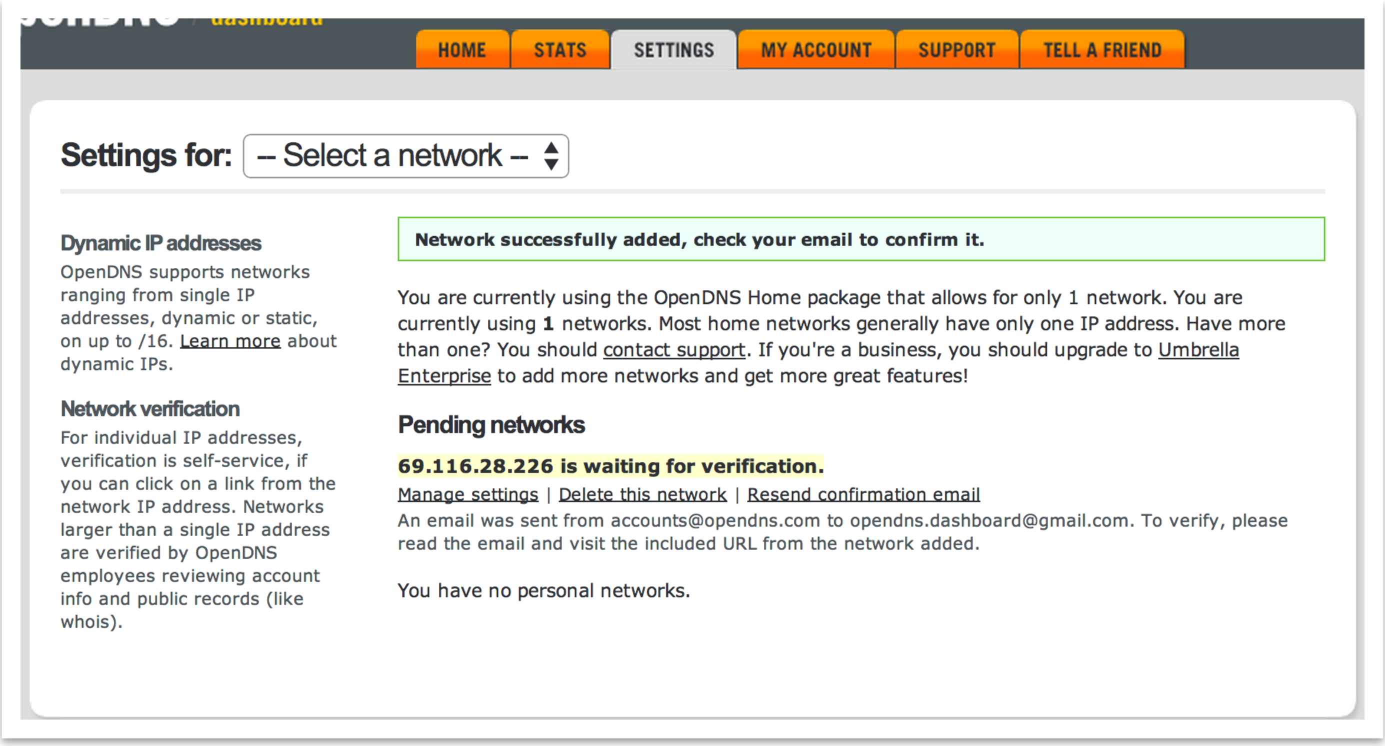


You've successfully added a network! Just a few more steps and you're home free.

1. Give it a friendly name: Home
   Something simple like "**Office**" or "**Home**" will do.
2. Is this a dynamic IP address? What is a dynamic IP address?.
   ☑ Yes, it is dynamic
3. Download the software and stay safe. The OpenDNS Updater software ensures that your OpenDNS preferences are preserved whenever your IP address changes.

Do not download the software under #3. The DD-WRT software on the router will handle the auto updating for you if you followed the router setup instructions above under "DDNS". If you have more questions regarding dynamic IP addresses please see Dynamic IP Addresses : Technical Detail and FAQ.

5. After you add your network you will see the screen below. Time to check your email to verify your IP address.



Settings for: – Select a network –

**Dynamic IP addresses**

OpenDNS supports networks ranging from single IP addresses, dynamic or static, on up to /16. Learn more about dynamic IPs.

**Network verification**

For individual IP addresses, verification is self-service, if you can click on a link from the network IP address. Networks larger than a single IP address are verified by OpenDNS employees reviewing account info and public records (like whois).

**Network successfully added, check your email to confirm it.**

You are currently using the OpenDNS Home package that allows for only 1 network. You are currently using **1** networks. Most home networks generally have only one IP address. Have more than one? You should contact support. If you're a business, you should upgrade to Umbrella Enterprise to add more networks and get more great features!

**Pending networks**

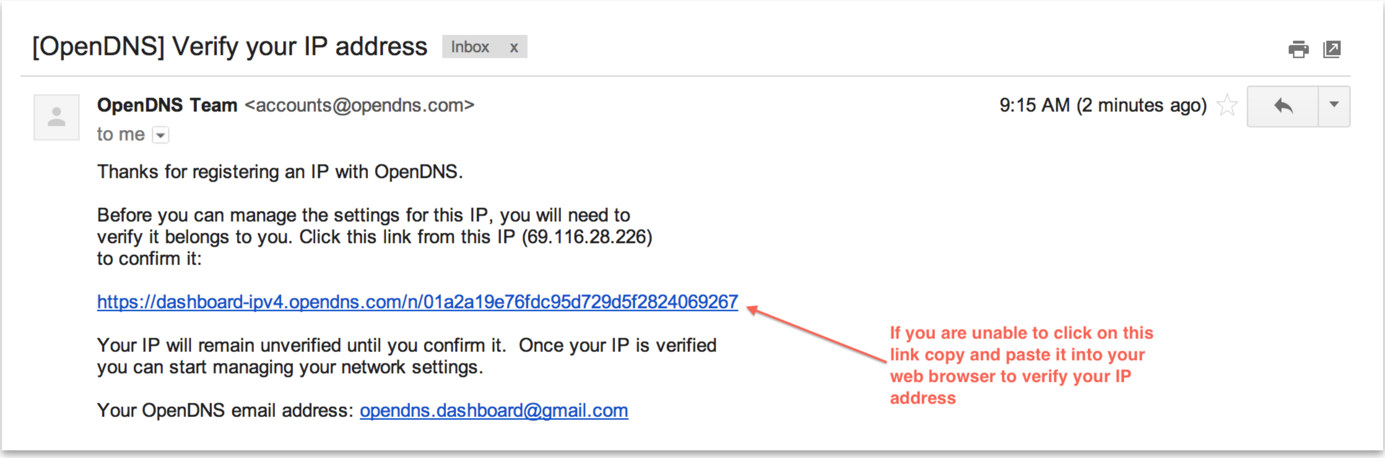
**69.116.28.226 is waiting for verification.**

Manage settings | Delete this network | Resend confirmation email

An email was sent from accounts@opendns.com to opendns.dashboard@gmail.com. To verify, please read the email and visit the included URL from the network added.

You have no personal networks.

6. You should receive an email that looks like the one below, once you click the link your IP address will be verified and you will be taken back to the dashboard.



[OpenDNS] Verify your IP address Inbox x

**OpenDNS Team** <accounts@opendns.com> 9:15 AM (2 minutes ago)

to me

Thanks for registering an IP with OpenDNS.

Before you can manage the settings for this IP, you will need to verify it belongs to you. Click this link from this IP (69.116.28.226) to confirm it:

https://dashboard-ipv4.opendns.com/n/01a2a19e76fdc95d729d5f2824069267

Your IP will remain unverified until you confirm it. Once your IP is verified you can start managing your network settings.

Your OpenDNS email address: opendns.dashboard@gmail.com

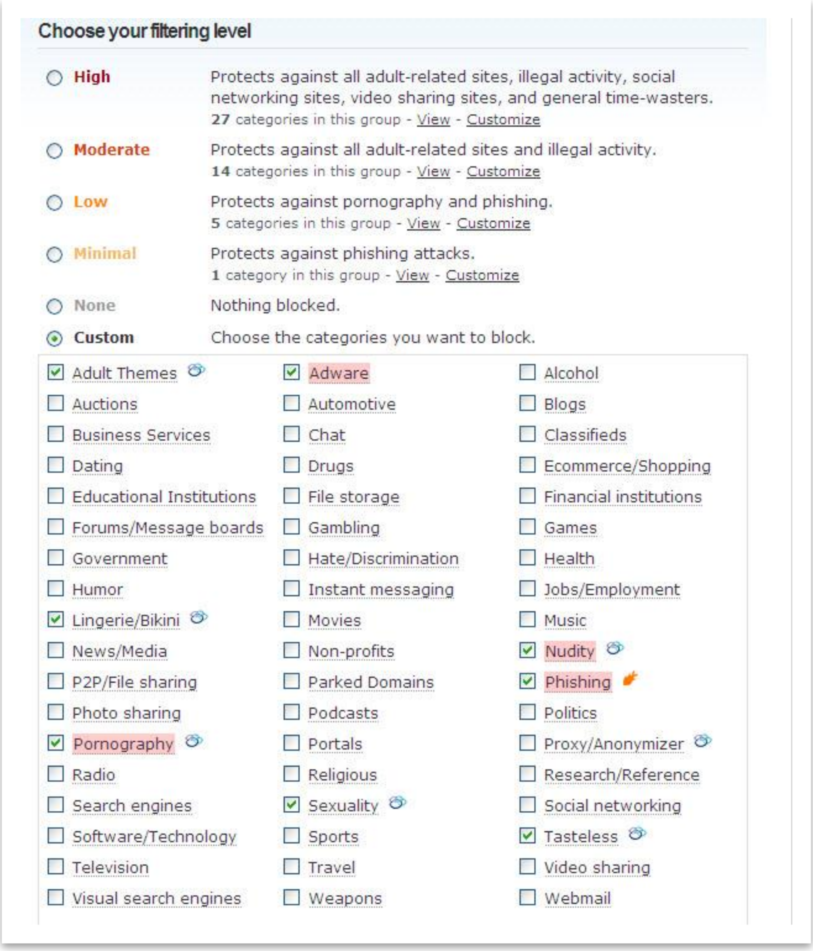
If you are unable to click on this link copy and paste it into your web browser to verify your IP address

7. Configuring Content Filtering Settings: After you have added a network, content filtering can be configured in the **Settings** tab. Click on the **Settings** tab and choose the network you added from the **Settings for:** drop down to open the **Web Content Filtering** menu for this network. In the **Choose your filtering level** settings you can choose from one of the levels that are pre-set or chose **Custom** to select the categories you would like to filter on your network. **Custom is powerful and recommended to filter specific categories like Social Media, File Sharing, and Webmail.**

***Based on our PG-13 presentation, especially for younger kids, please enable the following categories: Adult Themes, Alcohol, Dating, Lingerie/Bikini, P2P/File Sharing, Pornography, Adware, Chat, Drugs, Hate/Discrimination, Gambling, File Storage, Classifieds, Nudity, Phishing, Proxy/Anonymizer, Social***

***Networking, Tasteless, and Webmail (to block web-based email).*** This is the “magic” of the router. These categories will only apply to those connected to the “Kids Wireless” connection. “Home Wireless” is filtered via Norton ConnectSafe for general pornography and adware.

You can also manage individual domains to customize your filtering settings. For example, if you choose to block the **Lingerie/Bikini** category but would still like to shop at **victoriassecret.com** you can add **victoriassecret.com** to your **Never Block** list which will allow access to **victoriassecret.com** while blocking all other domains in that category.
For more information on content filtering please see: Web Content Filtering and Security.
For more information on configuring the **Manage individual domains section** please see: Getting Started: Blocking/Allowing Specific Domains with Whitelist/Blacklist.



Choose your filtering level

○ **High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.
27 categories in this group - View - Customize

○ **Moderate** Protects against all adult-related sites and illegal activity.
14 categories in this group - View - Customize

○ **Low** Protects against pornography and phishing.
5 categories in this group - View - Customize

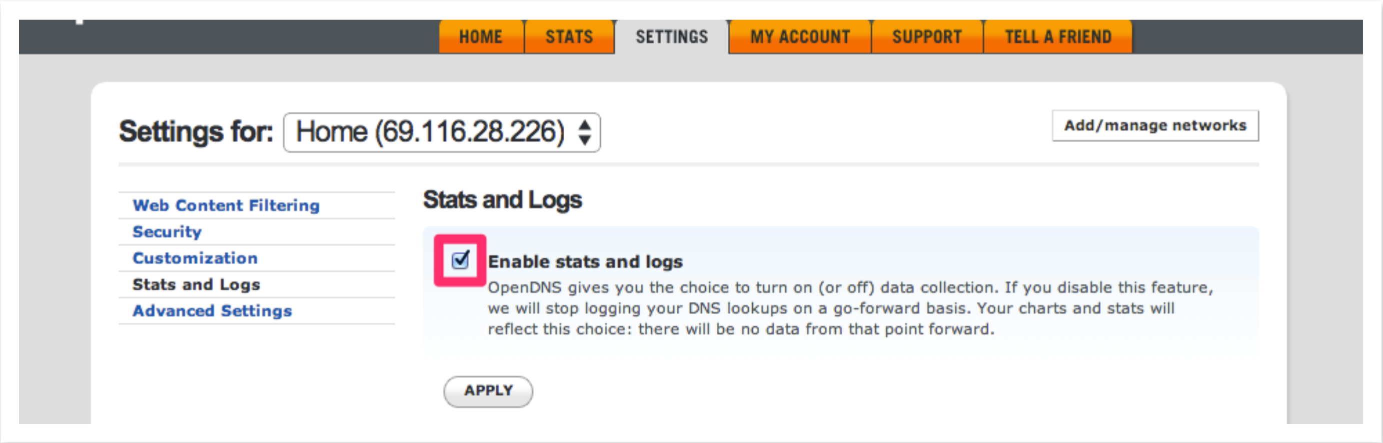
○ **Minimal** Protects against phishing attacks.
1 category in this group - View - Customize

○ **None** Nothing blocked.

● **Custom** Choose the categories you want to block.

| | | |
|---|---|---|
| ☑ Adult Themes | ☑ Adware | ☐ Alcohol |
| ☐ Auctions | ☐ Automotive | ☐ Blogs |
| ☐ Business Services | ☐ Chat | ☐ Classifieds |
| ☐ Dating | ☐ Drugs | ☐ Ecommerce/Shopping |
| ☐ Educational Institutions | ☐ File storage | ☐ Financial institutions |
| ☐ Forums/Message boards | ☐ Gambling | ☐ Games |
| ☐ Government | ☐ Hate/Discrimination | ☐ Health |
| ☐ Humor | ☐ Instant messaging | ☐ Jobs/Employment |
| ☑ Lingerie/Bikini | ☐ Movies | ☐ Music |
| ☐ News/Media | ☐ Non-profits | ☑ Nudity |
| ☐ P2P/File sharing | ☐ Parked Domains | ☑ Phishing |
| ☐ Photo sharing | ☐ Podcasts | ☐ Politics |
| ☑ Pornography | ☐ Portals | ☐ Proxy/Anonymizer |
| ☐ Radio | ☐ Religious | ☐ Research/Reference |
| ☐ Search engines | ☑ Sexuality | ☐ Social networking |
| ☐ Software/Technology | ☐ Sports | ☑ Tasteless |
| ☐ Television | ☐ Travel | ☐ Video sharing |
| ☐ Visual search engines | ☐ Weapons | ☐ Webmail |

8. Configuring Reporting/Statistics: If you would like statistics for your network, first you must Enable stats and logs on your network. To do so, click on the Settings tab, choose the network you added from the Settings for: drop down and click on Stats and Logs from the left hand menu. You will see the option to enable stats and logs, check the box and hit APPLY to enable stats as shown below:

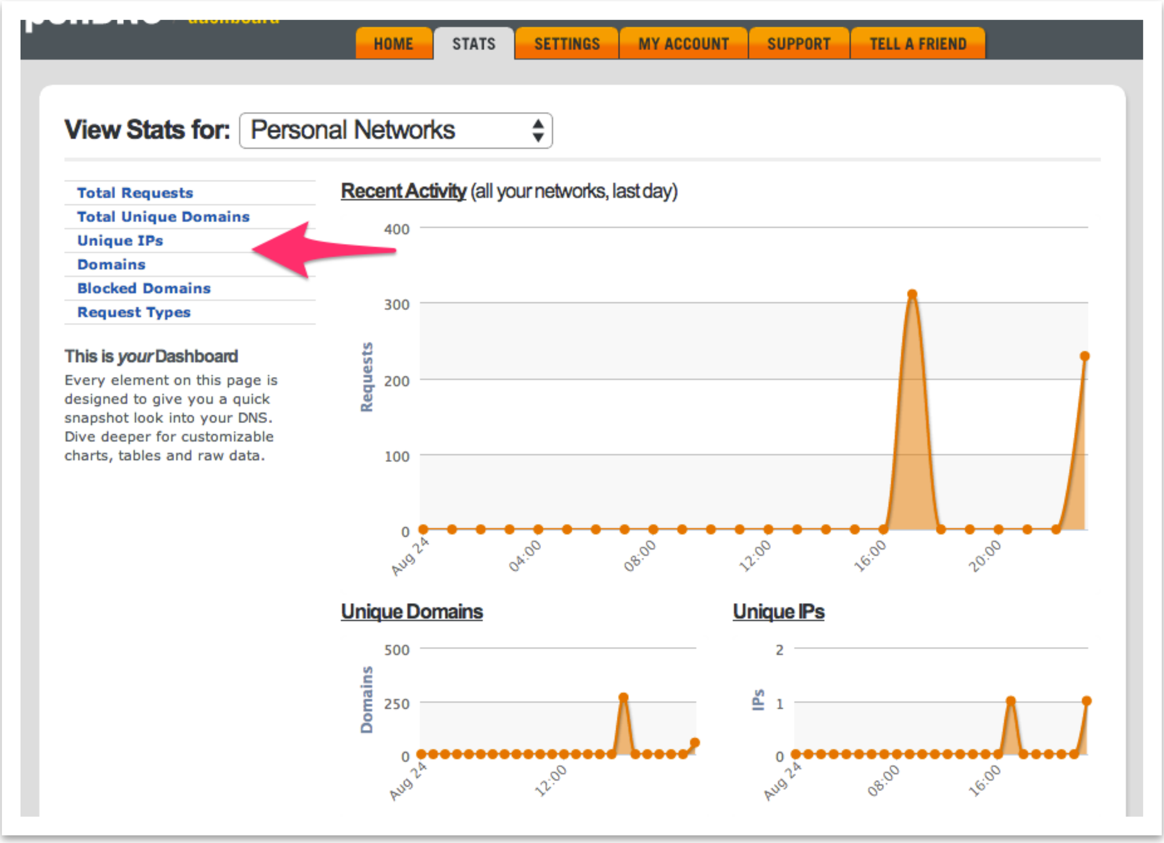


Settings for: Home (69.116.28.226)

Stats and Logs

☑ **Enable stats and logs**
OpenDNS gives you the choice to turn on (or off) data collection. If you disable this feature, we will stop logging your DNS lookups on a go-forward basis. Your charts and stats will reflect this choice: there will be no data from that point forward.

It can take up to 24 hours for stats to initially populate after you enable them, so if you don't see them right away don't fret they are coming! When stats begin to populate you can view them in the Stats tab. There are several different ways you can view your stats by choosing the options in the left hand menu:



View Stats for: Personal Networks

This is *your* Dashboard
Every element on this page is designed to give you a quick snapshot look into your DNS. Dive deeper for customizable charts, tables and raw data.

## Testing, FAQs, and more technical information

1. You made it! Well done. Now time to test. The “Home Wireless” network uses Norton ConnectSafe. To test your “Home Wireless” network go to playboy.com. IT SHOULD BE BLOCKED. As of 4/15/2015 (and since 2010) the playboy.com homepage is “safe” and does not have pornographic images on the homepage. Assuming you followed the steps above correctly, you should NOT get the playboy.com site and instead get the Norton ConnectSafe block page.

**2.** Thankfully OpenDNS has an easy testing website. To test OpenDNS, connect to the “Kids Wireless” connection and go to www.opendns.com/welcome. You should get a large checkmark indicating OpenDNS is setup correctly. If you do NOT get a large checkmark, you have something incorrect in the “Commands” section above (or see NOTE2 below) where you copied/pasted the large block of gray-colored code. Retry and reboot router and PC and retest on “Kids Wireless”.

**NOTE: OpenDNS will “work” with a green checkmark but that does NOT mean your low/medium/high/custom OpenDNS filtering settings are being applied. You must try a website that you know should be blocked in a category you specified and look for the OpenDNS block page instead of the website loading. For example, if you select “Custom” filtering profile and you then check off to block “Social Media”, this should block Facebook.com. When you go to facebook.com when using the “Kids Wireless” connection it should NOT load facebook.com and instead give you the OpenDNS block page.**

**If for example, you expected Facebook to be blocked based on your OpenDNS categories, and it is not AND you correctly get the checkmark indicator when you go to www.opendns.com/welcome, then your issue is with the “DDNS” section above. Your router is not correctly telling OpenDNS what your home internet connection IP address is and thus not applying your custom filtering categories. This could also be an issue if you did not properly put your modem into bridge mode.**

NOTE2: The commands above in “Commands” section that start with ”iptables” are what handle the DNS enforcement. If your kids try to specify their own DNS settings to bypass the filter the router with rewrite everything back to its local DNS server (called DNSMasq) which then forwards everything to either OpenDNS (for kids) and Norton ConnectSafe (for parents/Home Wireless).

## KEEP THIS PAGE - Checklist and Documentation

1. OpenDNS.com Username: ___________________________ Password: ____________________________

2. Router Configuration: http://192.168.1.1

   Router Username (root): ____________________________ Password: _____________________________

3. Parent/Home Wireless (≥8 characters): _____________________________

4. Kids Wireless Password (≥8 characters): _____________________________