COMPUTERWORLD
Networking & Internet

Hack DNS for lightning-fast Web browsing

Preston Gralla

May 23, 2007 (Computerworld) No matter how big the broadband pipe you use to surf the Web, it's not big enough. Everyone, whether they use a slowpoke dial-up modem or the fastest FiOS line, wants to surf faster.

There's a simple way you can get to Web sites faster, and it won't cost you a penny. You can hack the way your PC uses the Domain Name System (DNS), the technology underlying all Web browsing. It's far simpler to do than you might imagine, as you'll see in this article.

Understanding DNS

Before you start, it's a good idea to get a basic understanding of how DNS works. When you type in a URL such as *www.computerworld.com*, that URL needs to be translated into a numeric IP address that Web servers and Internet routers can understand. When you type in a URL, a DNS server does the translation, from *www.computerworld.com* to 65.221.110.98, for example.

DNS servers live on the Internet, and your computer contacts them with the request to do that translation, which is commonly called name resolution. When you use an ISP, your computer will automatically use the default DNS servers specified by your ISP; you typically don't need to set up DNS in any way. If you're on a corporate network, your systems administrator may have set you up to use specific DNS servers.

If there's a delay in contacting the DNS server, or if the DNS server takes too much time resolving the address, you'll face a delay in getting to a Web site. So even if you've got the world's fattest pipe, your Web surfing will be slowed down.

If you could speed up the name resolution in some way, you'd be able to speed up your Web surfing. And that's exactly what I'll show you how to do.

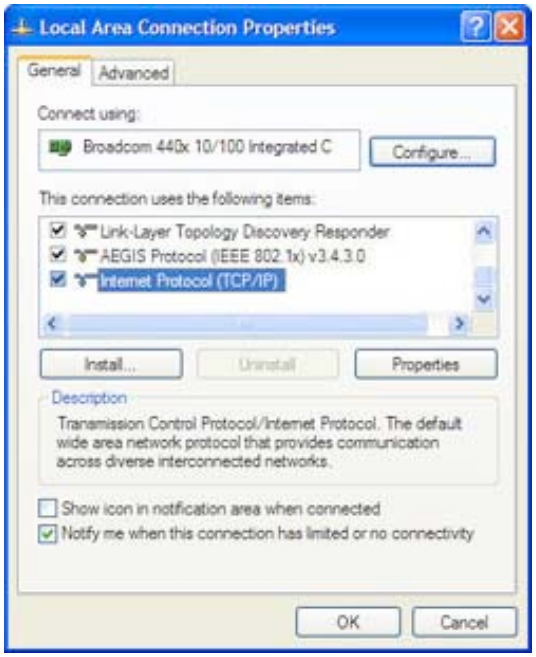
Speed up Web browsing with OpenDNS

Here's the simplest way to hack DNS to speed up your Web browsing: Use free, superfast DNS servers run by the **OpenDNS service** instead of your ISP's DNS servers. OpenDNS has a monstrously big DNS cache, with DNS servers around the world, so you'll be able to retrieve IP addresses from it more quickly than from your ISP's DNS servers.

As I'll explain a little later in this article, the service includes other benefits as well, such as letting you create browser shortcuts so that you could go to *www.computerworld.com*, for example, by just typing the letter **c** in your browser and pressing Enter.

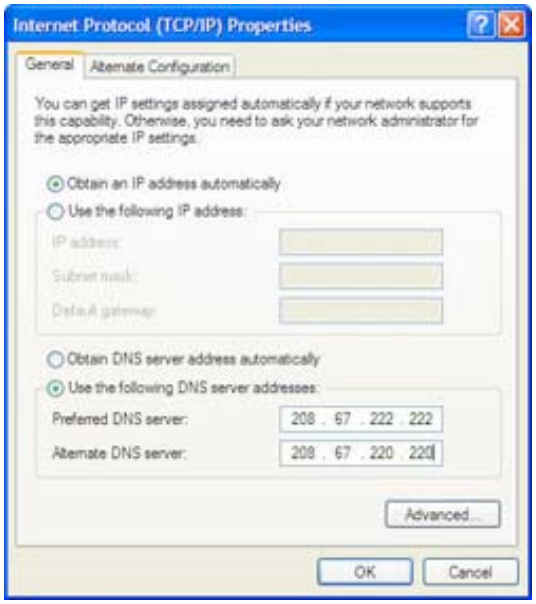
The addresses of the OpenDNS servers are 208.67.222.222 for a primary DNS server and 208.67.220.220 for a secondary server.

To use the OpenDNS servers, you'll have to tell your computer to use them. If you have Windows XP, first select Control Panel --> Network and Internet Connections --> Network Connections, right-click your network connection from the Network Connections window, and select Properties. A dialog box like that shown below appears.



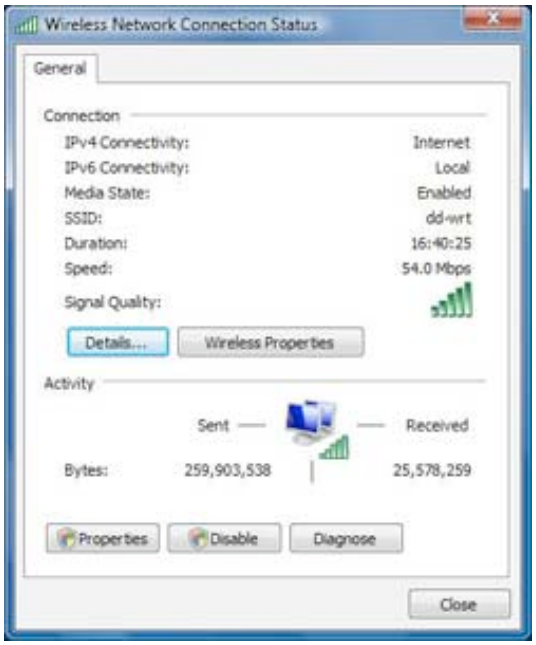
Highlight the Internet Protocol (TCP/IP) listing and select Properties in order to get to a dialog box that will let you use OpenDNS server. (Click image to see larger view.)

Scroll down to the Internet Protocol (TCP/IP) listing and select Properties. At the bottom of the screen, select "Use the following DNS server addresses." For the Preferred DNS server, enter this address: 208.67.222.222. For the Alternative DNS server, enter this address: 208.67.220.220. Click OK, and then click Close and Close again. Restart your PC in order for the settings to take effect. The figure below shows the screen filled out properly.



Telling your PC to use the OpenDNS servers. (Click image to see larger view.)

If you're using Windows Vista, select Control Panel --> Network and Internet --> Network and Sharing Center. Click the View Status link on the right side of the screen. The Local Connection Status screen appears, as shown in the figure below. Click Properties.



Click Properties in order to get to a dialog box that will let you use OpenDNS servers. (Click image to see larger view.)

You'll come to the same dialog box as you would for XP that lets you use the OpenDNS servers. Follow the same directions as for using OpenDNS on XP, and you'll be set.

When you configure a PC to use OpenDNS, only that PC will be able to use the OpenDNS servers. If you want all of the PCs on your network to use the servers, you can tell your router to use the OpenDNS servers, and then all of your PCs on the network will follow suit. That way, you won't have to configure each individual PC.

The way you do this will vary from router to router, and it changes according to whether you're using a router for a home office/small office or a larger corporate router. For a small office/home office router, you'll log into

your router, look for the DNS settings, and then use the OpenDNS settings of 208.67.222.222 for the primary DNS server and 208.67.220.220 for the alternative DNS server.

Whether you run a small network or larger network, you can get benefits beyond faster DNS. The service also gives you DNS management tools such as domain blocking. It also gives you statistics and charts about your network's DNS use.

On Linksys SRX 400 and many other Linksys routers, log into your router by going to the log-in page at 192.1681.1, using admin as the password and leaving the username blank. Scroll down the page until you come to the Static DNS 1 and Static DNS 2, as shown in the figure below. Click Save Settings. Restart your router and the PCs on your network, and they will begin using the OpenDNS DNS servers.

Change the DNS settings on this screen to use the OpenDNS servers for your entire network. (Click image to see larger view.)

If you run a corporate network and need help getting it set up, your best bet is to go to the **OpenDNS FAQ page**.

Note that OpenDNS may not work when using a virtual private network. For example, I wasn't able to get it to work using a Cisco VPN. And if you're on a corporate network, you should check with your systems administrator before using OpenDNS.

OpenDNS also lets you create shortcuts that let you visit Web sites by typing in a letter or group of letters instead of a full URL. To do that, you'll first need to register, which is free. After you do that, go to the site, log in, and click the Shortcuts link. On the page that appears, type in the shortcut text in the top box, and the URL in the bottom box and click Create Shortcut. From now on, when you type the shortcut text into your browser window, you'll be sent to the full URL.

You can also add the OpenDNS bookmarklet (found at the bottom of the page) to your browser and, in that way, create a shortcut no matter where you are on the Internet.

Creating a shortcut in OpenDNS. (Click image to see larger view.)

Speed up Web access with a HOSTS file

There's another way to speed up DNS -- by creating or editing a local HOSTS file on your own PC that contains URLs (also called hostnames) and their corresponding IP addresses. Windows will first look there to see whether there's an entry for the hostname, and if it finds it, it will resolve the address itself. That way, you won't have to go out to a DNS server and wait for the response before visiting a Web site.

The HOSTS file is a plain-text file you can create or edit with a text editor like Notepad. You should find an existing HOSTS file in C:\Windows\System32\Drivers\Etc\HOSTS in both Windows XP and Windows Vista. (In some versions of Windows, it may be located in C:\Winnt\System32\Drivers\HOSTS). The file has no extension; it is named only HOSTS. If you don't find one, create it in Notepad.

Open the HOSTS file in Notepad and enter the IP addresses and hostnames of your commonly visited Web sites, like this:
65.221.110.98 computerworld.com

Each entry in the file should be on one line. The IP address should be in the first column, and the corresponding hostname in the next column. At least one space should separate the two columns. When you're finished editing the file, save it to its existing location.

Make sure to check your HOSTS file regularly and keep it up-to-date, or else you might deny yourself access to certain Web sites. For example, if *www.computerworld.com* were to change its IP address but your HOSTS file kept the old, incorrect address, your browser would not be able to find the site.

Adjust Windows' DNS cache

To speed up DNS, Windows puts the DNS information into a local DNS cache on your PC when you visit a site. So when you want to go to a site, Windows first looks in its local DNS cache, called the resolve cache, to see whether the DNS information is contained there. That way, if it finds the information locally, it doesn't have to look in your HOSTS file or query a remote DNS server to find IP information. The cache is made up of recently queried names and entries taken from your HOSTS file.

The cache contains both negative and positive entries. Positive entries are those in which the DNS lookup succeeded and you were able to connect to the Web site. When Windows looks in the cache, if it finds a positive entry, it immediately uses that DNS information and sends you to the requested Web site.

Negative entries are those in which no match was found, and you end up getting a "Cannot find server or DNS" error in your browser. Similarly, when Windows looks in the cache and finds a negative entry, it gives you the error message without bothering to go out to the site.

Negative entries can lead to problems. When you try to make a connection to a site that has a negative entry in your cache, you'll get an error message, even if the site's problems have been resolved and it's now reachable.

You can solve this problem, though, using a Registry hack. By default, Windows caches negative entries for five minutes. After five minutes, they're cleared from your cache.

But if you'd like, you can force Windows not to cache these negative entries so that you'll never run into this problem. Run the Registry Editor by typing Regedit at a command prompt or the Windows Vista search box, and press Enter. Then go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters. Create a new DWORD value with the name NegativeCacheTime and give it a value of 0. (The value might already exist. If it does, edit its value to 0.)

The DWORD determines how much time, in seconds, to keep negative entries in the DNS cache. If you like, you can have the entries stay alive for one second by giving the DWORD a value of 1.

After you're done editing, exit the Registry. To make the change take effect, restart your computer, or flush your cache by issuing the command ipconfig /flushdns at a command prompt. The command will flush your DNS cache -- all the entries, both positive and negative, will be flushed -- and it will be empty until you start visiting Web sites. Negative entries, however, will not be added to the cache if you've given the DWORD a value of 0.

You can also use the Registry to control the amount of time positive entries are kept in the DNS cache. By default, they are kept for 24 hours. To change the default, go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters again and create a DWORD value called MaxCacheEntryTtlLimit. (If it's already present, just edit the value.) For the value, enter the amount of time you want the entry to remain, in seconds, making sure to use decimals as the base.

If you run into other DNS problems, see the related story, **"Fix your DNS problems."**

Note: Some of the content for this article was taken from my upcoming book **The Big Book of Windows Hacks** *and from* **Windows XP Hacks**.

Preston Gralla is a contributing editor for Computerworld *and the author of more than 35 books, including* **Windows Vista in a Nutshell**.

Related News and Discussion:

- **Is your DNS server configured wrong?**
- **Gartner: Hack contests bad for business**
- **$10k hack challenge winner says Vista's code more secure than Mac's**
- CJ Kelly: **Hacking Stupidity 101: Never hack from home**