

Code My Road

Programming Projects and Articles

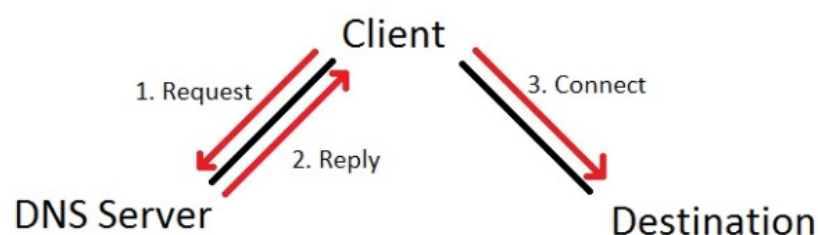
[Home](#) [About Me / Contact](#)

Monitoring Home Web Traffic With A Local DNS Proxy

Yiyuan Lee / August 31, 2013

What happens when you key in some domain name, say "banana.com", into your laptop's web browser and hit the enter button? Does your web browser automatically and magically connect to this domain, "banana.com"? How exactly does your web browser know where "banana.com" is even located at? To answer all these questions, we must first understand how the [Domain Name System \(DNS\)](#) works. With this understanding, we'll move on to see how we can make use of DNS to monitor your home web traffic.

Back to the basics



As shown in the above diagram, the following three steps are taken in order to resolve a domain name of a destination into its corresponding IP Address.

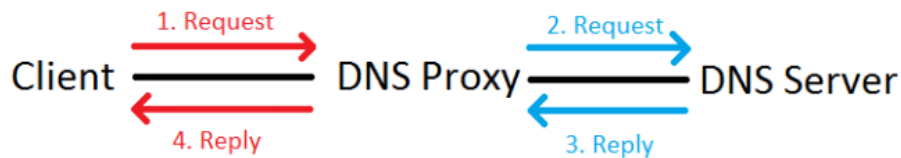
- **1. Request :** Client (your laptop) sends the domain name of the requested destination (banana.com) to a DNS Server.

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: [Cookie Policy](#).

Close and accept

That being said, all domain name resolution requests by a client has to go through a DNS Server before it can be resolved into an IP Address. But instead of connecting directly to an actual DNS Server, what happens if we make the client connect to a DNS Proxy (an intermediate device that acts as an actual DNS Server), which relays on the request to the DNS Server?

The DNS Proxy



The following steps are taken during the above exchange:

- **1. Request** : Client sends DNS request to DNS Proxy through UDP on port 53 of the DNS Proxy. This is because by convention, **most** DNS requests are received through UDP on port 53 of the DNS Server.
- **2. Request** : DNS Proxy forwards request to DNS Server through UDP on port 53 of the DNS Server.
- **3. Reply** : DNS Server replies to DNS Proxy with IP Address of destination.
- **4. Reply** : DNS Proxy forwards reply back to client.

As you can see, all domain name resolution requests will be intercepted by the DNS Proxy and then relayed on to the DNS Server. This implies that with a DNS Proxy, it's possible to monitor every single domain name resolution requests, which is really just web requests, that the client makes. Why, the DNS Proxy can even scan requests to filter out and invalidate banned domain names! But we'll focus just on the monitoring section today. Let's move on.

Modifying your home router

We've seen in the previous sections how introducing a DNS Proxy allows us to monitor web requests. But in order to make devices even connect to this DNS Proxy, it's necessary to modify the settings of your home router.

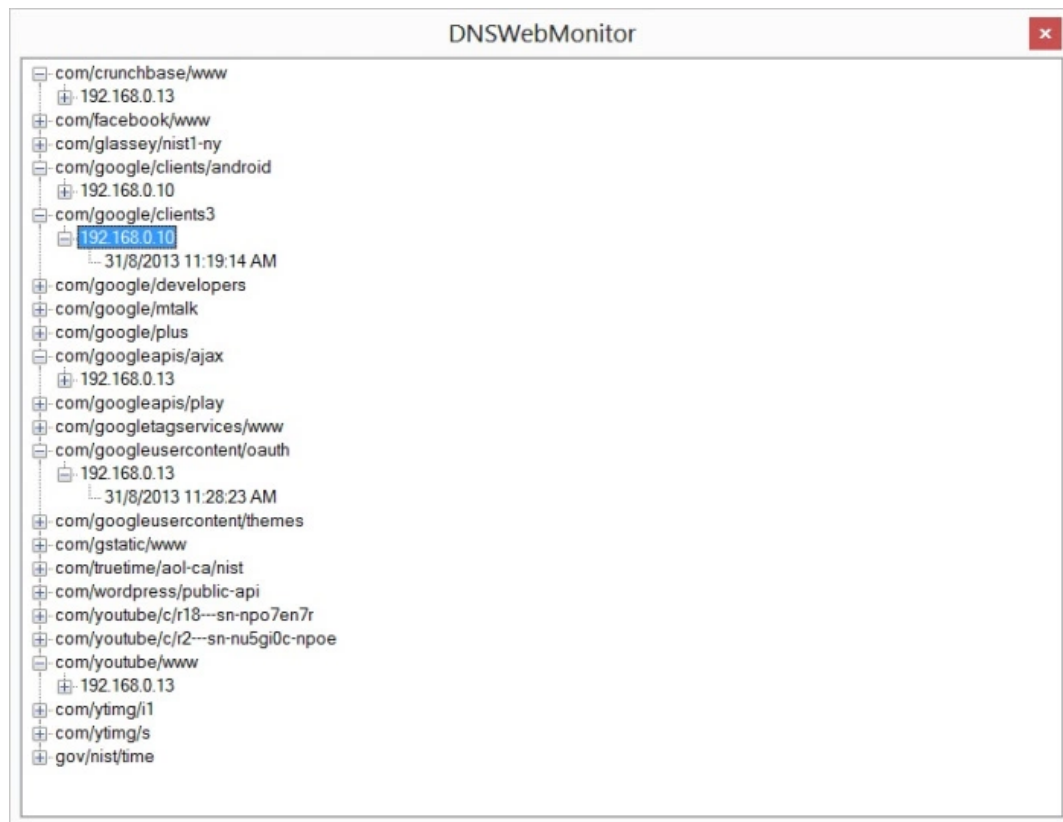
One function of a router is to tell connected devices which DNS Servers to send requests to, and this is done by modifying the DNS settings on the router to point to the DNS Proxy. This is done by obtaining the local IP Address (through ipconfig in CMD) of your DNS Proxy (which is your laptop/PC) and entering it into the DNS settings on your router.

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: [Cookie Policy](#).

Close and accept

Results

The demo application that I've written in C# listens for incoming UDP request on port 53 and relays them to Google's DNS Server – "Google Public DNS", whose IP Address is 8.8.8.8. The application also outputs, on a GUI, the monitored home web traffic. Below shows some images of the application in action.



Downloads

Note: .NET Framework 4.0 or above is required to run the PC binary program. Visual studio 2012 is required to open the PC source files.

Demo App Sources – <https://hostr.co/OXYofngQHMXk>


Demo App Binaries – <https://hostr.co/DFp2Xzg2tbdV>


Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: [Cookie Policy](#)


Close and accept

Advertisements

Share this:

 Google

 Facebook

 Twitter

Like

Be the first to like this.

August 31, 2013 in Articles. Tags: dns proxy, monitor traffic

Related posts



P2P File Transfer over TCP



PC Controlled Lego Car over Bluetooth

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: [Cookie Policy](#).

Close and accept

[← How to write a Diamond Dash Bot](#)[P2P File Transfer over TCP →](#)

One thought on “Monitoring Home Web Traffic With A Local DNS Proxy”

Pingback: [Surviving Tips:Performance e DNS | The Puchi Herald Reblog](#)

Leave a Reply

Enter your comment here...

Posts by Month

[April 2015](#) (1)

[March 2015](#) (1)

[May 2014](#) (2)

[March 2014](#) (1)

[November 2013](#) (1)

[August 2013](#) (3)

[July 2013](#) (1)

[June 2013](#) (1)

[April 2013](#) (2)

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: [Cookie Policy](#).

Close and accept

[Blog at WordPress.com.](#)



Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: [Cookie Policy](#).

Close and accept