namehelp: Intelligent Client-Side DNS Resolution

John S. Otto, Mario A. Sánchez, John P. Rula, Ted Stein, and Fabián E. Bustamante
Northwestern University
{jotto, msanchez, john.rula, ted.stein, fabianb}@eecs.northwestern.edu

ABSTRACT

The Domain Name System (DNS) is a fundamental component of today's Internet. Recent years have seen radical changes to DNS with increases in usage of remote DNS and public DNS services such as OpenDNS. Given the close relationship between DNS and Content Delivery Networks (CDNs) and the pervasive use of CDNs by many popular applications including web browsing and real-time entertainment services, it is important to understand the impact of remote and public DNS services on users' overall experience on the Web. This work presents a tool, *namehelp*, which comparatively evaluates DNS services in terms of the web performance they provide, and implements an end-host solution to address the performance impact of remote DNS on CDNs. The demonstration will show the functionality of *namehelp* with online results for its performance improvements.

Categories and Subject Descriptors

C.2.4 [**Computer Communication Networks**]: Distributed Systems

Keywords

Domain Name System, Content Delivery Networks

1. MOTIVATION

The Domain Name System (DNS) is a critical component of today's Internet. DNS provides a distributed lookup service primarily used to resolve human-readable machine names to Internet Protocol addresses. The pervasiveness of the Web and the Web's dependence on DNS to resolve the hostname portion of URLs has further accentuated its importance [7].

Recent years have brought radical changes to DNS with the increasing use of remote DNS and the growth of public DNS services such as OpenDNS, UltraDNS and Google DNS. Public DNS services promise higher reliability and faster lookup times as well as a number of security features (e.g. phishing protection).

Several studies have shown the potential advantages of a "personalized" selection of DNS servers based on responsiveness [1,3,4]. The close relationship between many web applications and DNS demands a careful analysis of the impact of remote and public DNS usage on users' web experience. An increasing fraction of the Web relies on Content Delivery Networks (CDNs) for scalability and performance.

In a survey of CDN usage by popular websites, we found that 75% of the top 1000 sites (as ranked by Alexa) use a CDN. CDNs cache content at several replica servers throughout the network and redirect clients to a nearby replica for low latency, high bandwidth access to content. The selection of a replica to serve a given client's request is commonly done based on different features including the client's approximate location, and network and server loads. To approximate the client's location, CDNs adopt the location of the client's DNS resolver as a proxy on the assumption that clients are near their DNS resolvers (DNS-based redirection). The recent growth of public DNS services and the use of remote DNS by ISPs break this assumption potentially resulting in worse end-to-end web performance.

2. END-HOST SOLUTION: namehelp

The potential negative impact of remote DNS usage on web performance motivates the recently proposed EDNS0 extension [2]. This extension, put forward by a collaboration of several CDNs and DNS service providers [6], allows DNS recursive resolvers to pass along clients' subnet information that could be used by CDNs to improve replica server selection. A key challenge to this approach is adoption, as it requires the commitment of both CDN and DNS services to be effective.

We present *namehelp*,[1] an end-host based system that comparatively evaluates the CDN and web performance obtained when using different DNS services, helping users to choose the best DNS service. In addition, it implements a client-side technique for obtaining good CDN and web performance even when using remote DNS services.

namehelp has two major components: the DNS proxy for improving web performance with remote DNS and a DNS server recommendation engine; we discuss each in turn.

2.1 DNS proxy functionality

namehelp functions as a transparent DNS proxy running on the user's local machine. After installing *namehelp*, users have only to configure "localhost" as their primary DNS server to start using it.

As the machine's primary DNS server, *namehelp* receives the full stream of DNS queries coming from the operating

SIGCOMM'12, August 13–17, 2012, Helsinki, Finland.
ACM 978-1-4503-1419-0/12/08.

[1] http://aqualab.cs.northwestern.edu/projects/namehelp

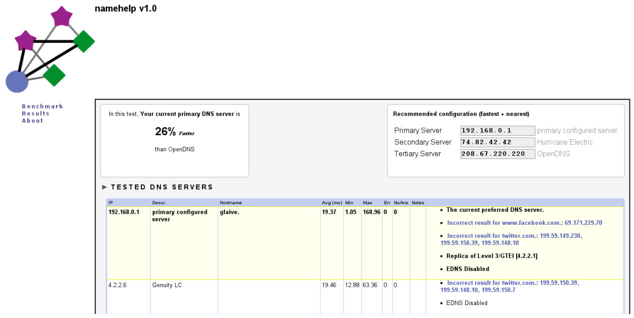

Figure 1: The *namehelp* DNS configuration recommendation interface, showing a ranked list of DNS servers.

system. By default, it simply passes on these queries to the configured recursive DNS servers such as the DHCP-provided DNS configuration or a specific IP address, such as Google's DNS server (8.8.8.8).

When the proxy receives the DNS answer from the recursive resolver, it examines the response to determine whether there was a redirection to a CDN by looking for a canonical name (`CNAME`) record in the reply. In the simple case – when no CDN redirection occurred – *namehelp* returns the answer directly to the operating system. However, if a CDN redirection took place, *namehelp* discards the response and directly queries the CDN's authoritative DNS server for the same `CNAME` record, returning the answer from the second query. Since the client queries the CDN directly, the CDN knows the actual location of the client resulting in potentially improved server selection and better performance.

namehelp acts also as a local DNS cache and prefetches frequently-requested queries for improved performance. This caching also allows us to skip the queries to other resolvers for names that are known to be CDN redirections, reducing the total overhead in the vast majority of cases to a fraction of a millisecond of local processing.

2.2 Configuration recommendations

To enable users to make an informed decision regarding which DNS server to configure, *namehelp* periodically runs a battery of tests that compare DNS servers. The result is a ranked list of DNS servers, as shown in Fig. 1, which tells users which DNS service is best in terms of several factors, including responsiveness and the quality of CDN redirections. We incorporate code from the popular *namebench* DNS benchmarking utility [5] for this task. *namehelp* schedules tests periodically to produce suggested configurations based on both DNS performance and HTTP performance.

Since each user has a unique set of websites she visits, *namehelp*'s benchmarking tests personalize the list of sites to test based on the user's habits, incorporating information from the user's browser history. As a result, the DNS configuration recommended by *namehelp* is personalized for best web performance.

After running the tests, *namehelp* generates a report that includes the ranked list of DNS servers and justifications for its results. A pane of the user interface is dedicated to presenting the current and historical reports to the user.

Once the report has been generated, *namehelp* has two options for acting on the results: manual or automatic configuration. With manual configuration, the user simply examines the results and decides which server to use. However, the best DNS service for a user may vary over time for several factors, including changes in the sites a user visits to variations in the performance of the selected DNS service (e.g. due to fluctuations in load). To handle this scenario, *namehelp* can be configured to automatically update the user's DNS configuration to match the recommendation from the latest test.

3. DEMONSTRATION

Our demonstration of *namehelp* will include the following elements:

- Online analysis of the DNS proxy's performance improvement
- Fine-grained tool to examine the DNS proxy's behavior
- Examples of varying web browsing patterns and their impact on recommended DNS
- Results of running benchmarking tests in several different network environments

Acknowledgements

We would like to thank the reviewers for their comments. This work is supported by the National Science Foundation through Awards CNS 0917233 and CNS 0855253, and by a generous Google Research Award.

4. REFERENCES

[1] B. Ager, W. Mühlbauer, G. Smaragdakis, and S. Uhlig. Comparing DNS resolvers in the wild. In *Proc. of IMC*, 2010.

[2] C. Contavalli, W. van der Gaast, S. Leach, and E. Lewis. Internet-draft: Client subnet in DNS requests, 2012. `http://tools.ietf.org/html/draft-vandergaast-edns-client-subnet-01`.

[3] C. Huang, D. A. Maltz, A. Greenberg, and J. Li. Public DNS system and global traffic management. In *Proc. of IEEE INFOCOM*, 2011.

[4] R. Khosla, S. Fahmy, and Y. C. Hu. Content retrieval using cloud-based DNS. In *Proc. of IEEE Global Internet Symposium*, 2012.

[5] namebench. http://code.google.com/p/namebench/.

[6] The Global Internet Speedup. A Faster Internet. `http://www.afasterinternet.com`.

[7] M. Walfish, H. Balakrishnan, and S. Shenker. Untangling the Web from DNS. In *Proc. of USENIX NSDI*, 2004.