BLG 433E

COMPUTER COMMUNICATIONS

CRN: 12337

REPORT OF PRESENTATION

Submission Date: 11.12.2014

Group Members:

Mustafa UÇAR	040100113
Tuğrul YATAĞAN	040100117
Emre GÖKREM	040100124

ON MODERN DNS BEHAVIOR AND PROPERTIES

Title:	ACM SIGCOMM Computer Communication Review Volume 43 Issue 3, July 2013	
Authors:	Thomas Callahan	Case Western Reserve University, Cleveland, OH, USA
	Mark Allman	International Computer Science Institute, Berkeley, CA, USA
	Michael Rabinovich	Case Western Reserve University, Cleveland, OH, USA
Pages:	7-15	
Date:	2013-07-01	
Sponsor:	SIGCOMM ACM Special Interest Group on Data Communication	
Publisher:	ACM New York, NY, USA	
	ISSN: 0146-4833 doi>10.1145/2500098.2500100	

Abstract

In this paper online content providers including Amazon, Google and Microsoft, and by network game researchers have quantified the impact of network latency on user behavior. DNS is an important part of that latency, both in contributing to initial connection setup latency but also in picking a server that has low network distance and low load for the client to use. A number of measurement studies of DNS behavior on the Internet have been published in the past, this paper is relatively recent one. The authors have studied 14 months of data from a 90 home neighborhood in the US, served by bi-directional 1 Gbps fiber links. This data includes 200 million DNS queries and 1.1 billion flows. There are a number of notable findings in this paper. 63% of hostnames were requested only once throughout the 14 month window. Google's public DNS resolver served only 1% of queries. 75% of hostnames mapped to only 1 IP address, and those tended to not be optimized for geographic locality to the client. Two-thirds of DNS transactions completed in under 1ms, but 25% took between 10ms and 1s. 40% of DNS responses went unused, perhaps as a result of DNS prefetching.

1. Introduction

Domain Name System (DNS) is a distributed, hierarchical naming system. The DNS calls for organizational name servers to hold the authoritative binding between IP addresses and hostnames only for their own hosts. Clients then query for this mapping as needed. This provides human-friendly hostnames without the logistical burdens of maintaining a single master list of all hosts on the network. Over the years, the DNS infrastructure has grown and morphed in a number of dimensions. For instance, DNS is commonly used as a query mechanism for various blacklists of compromised or otherwise misbehaving actors on the Internet. Also, DNS supports named services as well as hostnames to support discovery of transport port numbers.

At its core DNS is a simple protocol with requests and responses each generally contained in a single UDP packet. Further, resolving a hostname requires only a small number of transactions. For instance, finding the IP address corresponding to www.google.com first requires finding the authoritative servers for ".com", and then for ".google.com" and finally looking up the IP addresses of "www.google.com". The results from each step can be cached such that future lookups may require even fewer steps.

In this paper authors describe an initial study of modern DNS behavior as observed from the vantage point of clients within a small residential network over a recent 14 month span. While some of analysis in the paper is a reappraisal of previous work conducted by others researchers.

2. Research Datasets And Methodology

For this study researchers monitor DNS traffic within the "**Case Connection Zone**", which is an experimental network that connects roughly 90 homes in a neighborhood adjacent to Case Western Reserve University to the Internet via bi-directional 1 Gbps fiber links. The connections from each house come together in a switch. They have a packet-level monitor that receives all traffic via a mirroring port on all switches.

3. DNS Requests

Communication across the Internet generally starts with a DNS query from a user facing device. Some applications continue to heavily rely on DNS over the course of their operation, while others only use DNS for bootstrapping. Fundamentally the request to resolve a hostname into an IP address is straightforward and the DNS protocol is likewise uncomplicated.

DNS query types in studied dataset, type A queries (A records are used to map a domain name to an IPv4 address.) for IPv4 addresses associated with some hostname are the most prevalent with over 87% of the requests per month at the median. The PTR (PTR records are also called Reverse DNS records.) lookups appear to be predominantly Bonjour discovery traffic. Researchers also find that AAAA lookups (AAAA records are used to map a domain to an IPv6 address.) for IPv6 addresses constitute a median of 4.1% of the queries per month even though they find almost no actual IPv6 use by CCZ hosts. Researchers guess that, this is caused by some operating systems making A and AAAA queries simultaneously regardless of whether or not the host intends to use IPv6.

Finally, researchers note that roughly 97% of the DNS requests they observe traverse one of the two local resolvers provided for CCZ clients. The primary resolver is used for approximately 81% of the overall requests and the secondary resolver handles 16%. These resolvers are not specifically for CCZ users, but are more broadly used within the Internet service provider supplying access to the CCZ network. Google's public DNS resolver handles just over 1% of the requests are observed in paper. The remaining 2% of the requests are dealt with by myriad resolvers.

4. DNS Responses

a. TTLs

Time-To-Live (TTL) associated with hostnames in DNS responses. The TTL is assigned by the authoritative DNS server and indicates the time period for which the response is valid. The TTL aims to provide consumers with the ability to cache the result of a lookup such that future requests for the same name can be handled

locally, while at the same time allowing the name-to address associations to expire at some future point such that they can be changed. Longer TTL values allow for higher cache hit rates (and therefore decreased DNS traffic), while lower TTL values allow a service provider more agility in terms of changing their mappings and directing traffic.

Popular TTL values in the CCZ network, 20 seconds, 60 seconds, 1 hour, etc. Researchers find a median TTL of 5 minutes and that only roughly 1% of the TTLs exceed one day. Researchers also find roughly 40% of the hostnames have TTLs of at most 1 minute.

b. Equivalent Answers

Individual DNS responses may contain multiple mappings in response to a single query for two reasons. First, multiple IP addresses give clients recourse if they cannot communicate with a particular IP address. Second, this aids load balancing across a set of replicas as recursive DNS servers will rotate the order of the IP addresses returned when serving records from the cache.

c. Proximity

Researchers tried to understand the geographic distance between returned IP addresses and the requesting user device. It is well known that popular services attempt to provide content from nearby servers and that directing traffic via DNS is a popular way to drive clients to close servers. They use a geolocation database from MaxMind to map IP addresses to locations at a city-level granularity. Since DNS responses can have multiple answers researchers consider the geographic distance to each position in the DNS response independently. For each DNS response they calculate the average distance to each position in the response. For all such averages they then compute the quartiles for each position and each DNS response size. For instance, for responses with two IP addresses researchers calculate the quantiles for the first and second positions independently. They determine the quantiles for DNS responses containing 1 to 4 IP addresses. Researchers find the distance quantiles are the same regardless of position in the DNS response.

5. Transmission

In researcher's first observation is that roughly two-thirds of the transactions complete in under 1 msec. This suggests that these DNS requests are being serviced from the cache at the CCZ resolver. Another roughly 10% of the transactions take approximately 10 msec. These transactions are likely associated with traffic to nearby institutions. The third region of the plot shows that the longest 25% of the transactions are well spread across the interval between 10 msec and 1 second. These are transactions that have to make their way through the global DNS ecosystem to a variety of authoritative DNS servers around the world.

6. Utilizing Responses

a. Use of DNS Responses

Researchers stated that, DNS responses often contain more than one IP address for a particular hostname. In principle, these IP addresses are equivalent and clients can use any one of the set. Researchers then tried to understanding which IP addresses clients actually do use in subsequent communication.

They find that more than 60% of the connections are made to the first IP address listed in the response across all response sizes with the exception of responses with five addresses and, even in that case the first address is used in just under 60% of the subsequent connections. Further, for responses with 3 to 6 IP addresses the use of all but the first position is fairly uniform distribution.

b. TTLs

Researchers next focus on how well clients honor the TTLs given in DNS responses. Their previous work observes that around 47% of clients and their resolvers in combination violate the TTL and that most violations extend beyond two hours after the mapping expires. Further, findings shows that 8–30% of connections utilize expired DNS records across several datasets from different vantage points. In the dataset they find that 13.7% of TCP connections use addresses from expired DNS responses.

While roughly 55% of hostnames have TTLs of at most 350 seconds, researchers find that 68% of connections and 87% of traffic volume is associated with DNS records with TTLs of at most 350 seconds. Further, while 80% of hostnames have TTLs of at most one hour, they find that 85% of connections and 95% of bytes associate with DNS TTLs of at most one hour.