Review of Domain Name System

1Simar Preet Singh and 2Raman Maini
1Research Scholar, University College of Engineering,
Punjabi University, Patiala-147002 (INDIA)
2Associate Professor, University College of Engineering,
Punjabi University, Patiala-147002 (INDIA)

ABSTRACT

This paper focuses on performance optimization of network by using co-located domain name systems. The study involves understanding of the flow of traffic from source to the destination, load balancing among servers evenly in order to provide sufficient quality of service to end-users, and the need of co-located DNS is because it picks data from the nearby available servers. Performance of co-located DNS will be measured and analyzed so that better solution can be proposed and various tools for analyzing and monitoring are to be used for measurement and analysis purpose. They can measure and analyze the response time for the input, latency, bandwidth, flow of traffic, delays etc. so that the promising solution in terms of performance, scalability and availability may be suggested.

Keywords

DNS, Colocated DNS, scalability, performance.

I. INTRODUCTION

The “Domain Name System” was created in 1983 by Paul Mockapetris. The Internet users use DNS to reference anything by name on the Internet. The mechanism by which Internet software translates names to addresses and vice versa is called the domain name server. IP assigns 32-bit addresses to hosts (interfaces). Binary addresses are easy for the computers to manage. All applications use IP addresses through the TCP/IP protocol software [11, 12]. IP addresses are difficult for humans to remember. Thus, the domain name systems are important. Domain names comprise a hierarchy so that names are unique, easy to remember.

Domain Name: A domain name is the sequence of labels from a node to the root, separated by dots (“.”s), read left to right. The example of domain name is as follows:

- punjabiuniversity.ac.in
- google.com
- yahoo.com
- microsoft.com
- rediffmail.com

Sub-domain: One domain is a sub-domain of another if its domain name ends in the other‟s domain name. Consider the website

punjabiuniversity.ac.in

In this, punjabiuniversity.ac.in is a subdomain of

- ac.in

which is futher a sub-domain of

- in

In the same way, google.com is a sub-domain of com.

II. DNS NAMING STRUCTURE

The DNS is arranged as a hierarchy[6]. At the top of the hierarchy is the root domain "." which is administered by the Internet Assigned Numbers Authority (IANA)[1]. Administration of the root domain gives the IANA the authority to allocate domains beneath the root. The process of assigning a domain to an organizational entity is called „delegating‟ and involves the
administrator of a domain creating a sub-domain and assigning the authority for allocating sub-domains of the new domain the sub-domain's administrative entity. eg.

fred.abcd.edu.au

is the name of a host system (fred) within the abcd University, an educational (edu) institution within Australia (au).

The majority of country domains are sub-divided into organizational-type sub-domains[7,8]. In some countries two character sub-domains are created (eg. ac.nz for New Zealand academic organisations) and in others three character sub-domains are used (eg. com.au for Australian commercial organisations)[2]. Regardless of the standard adopted each domain may be delegated to a separate authority. Thus, DNS Naming Structure consists of as follows:

- Top level domains (TLDs) - These are defined by

global authority. Top level domains are as follows:

- com
- org
- edu

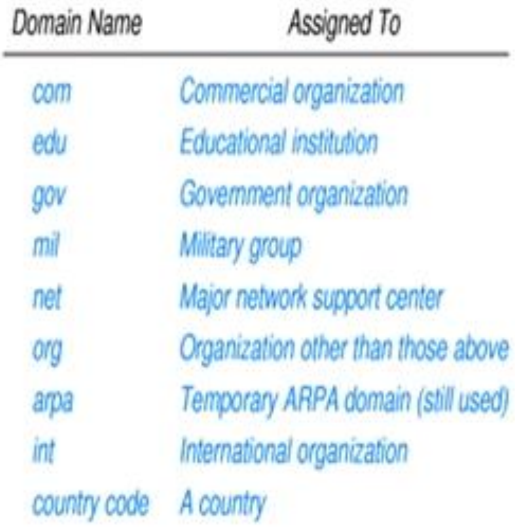
- ccTLD: These are the country code TLDs. Some

of the ccTLD‟s are as follows:
- in

- uk
- as

- 2nd Level Domains: 2nd Level domains are as follows:
  - ac.in
  - google.com

The various Top-Level Domains are as follows:



Domain Name	Assigned To
com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support center
org	Organization other than those above
arpa	Temporary ARPA domain (still used)
int	International organization
country code	A country

Table1: Top-Level Domai ns DNS Name space:DNS name space is the hierarc hical structure of the domain name tree. It is defined such that the names of all similar components must be similarly structured, but similarly identifiable[9,10]. The full DNS name must point to a particular address.

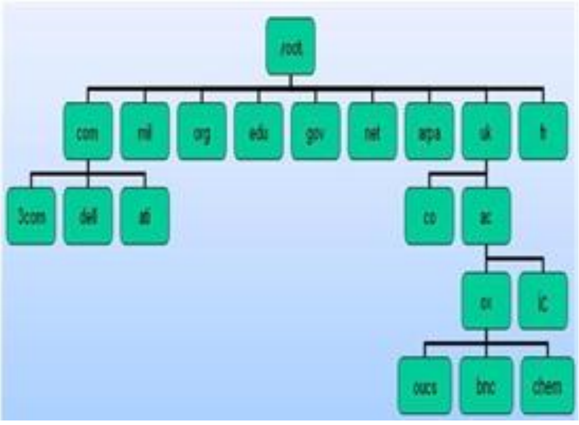


Fig 1: DNS Namespace

The above hierarchical tree of domains contains:
- Root

- Top level domains (gov, edu, com, fr, org, uk etc.)

- Some countries have sub-domains denoting organisation type (eg. ac.uk, co.uk)

Sub-domains generally for specific organisations (e.g. dell.com,

microsoft.com etc.)

Sub-domains within organisation (eg.

oucs.ox.ac.uk)

Technically, a domain is the part of the name space at or below the domain name identifying the domain.

Consider the following image of DNS namespace of the Internet:

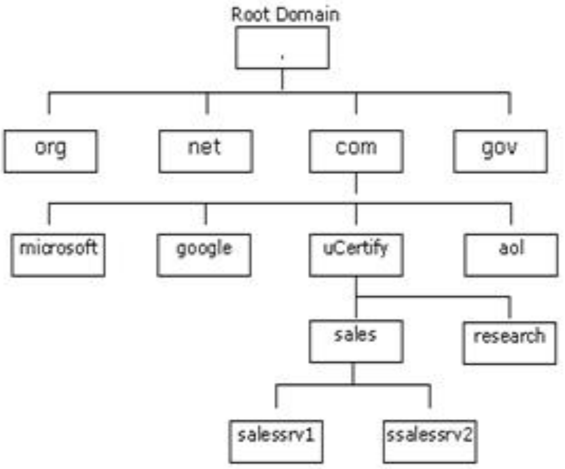


Fig. 2: DNS Namespace

The salessrv1 and salessrv2 are host names of the hosts configured in the sales.ucertify.com domain. The fully qualified domain name (FQDN) of the host salessrv1 is salessrv1.sales.ucertify.com. No two hosts can have the same FQDN.

Country Code Domains: A country code top-level domain (ccTLD) is an Internet top-level domain generally used or reserved for a country, a sovereign state, or a dependent territory. Some of the concepts about the country code domains are as follows:

- Top level domains are US-centric.

- Geographic TLDs used for organizations in other

countries:

TLD	**Country**
.uk	United Kingdom
.fr	France
.ye	Yemen

- Countries define their own internal hierarchy: gov.ye, org.ye, net.ye, edu.ye and com.ye are used for organizations in Yemen

Second-Level Domains:

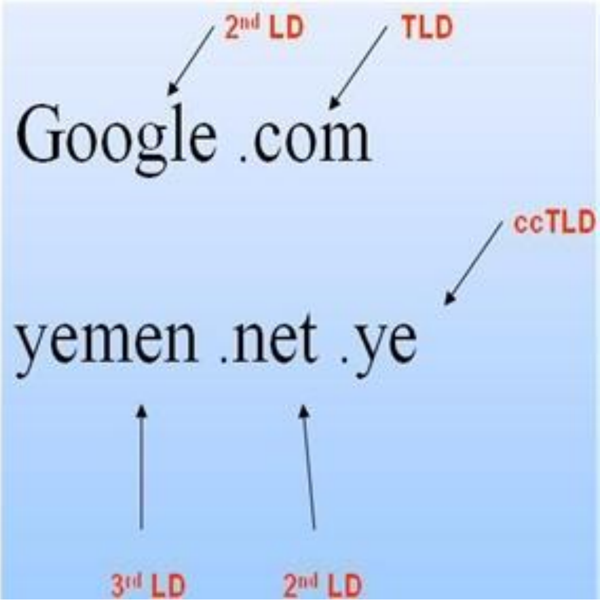


Fig 3: DNS Naming Structure Example

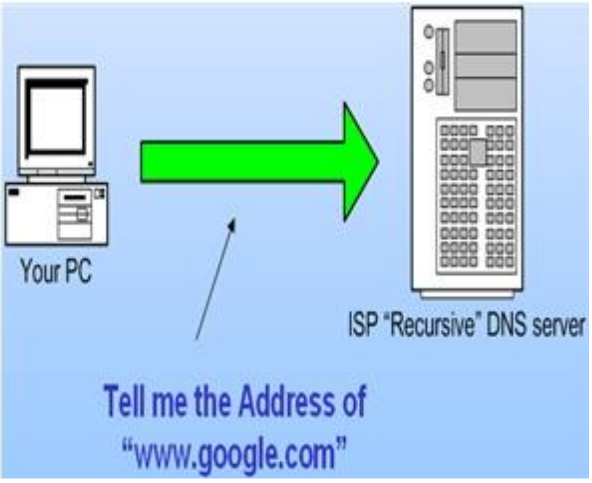


Fig 4: Step 1 DNS Servers work

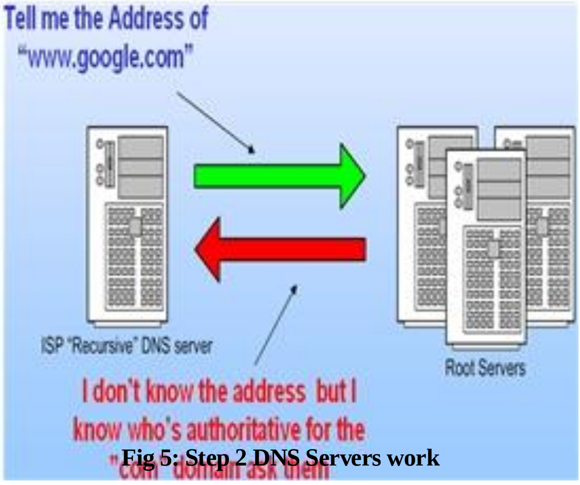

Tell me the Address of
"www.google.com"
ISP "Recursive" DNS server
Root Servers
I don't know the address but I
know who's authoritative for the
"com" domain ask them

Fig 5: Step 2 DNS Servers work

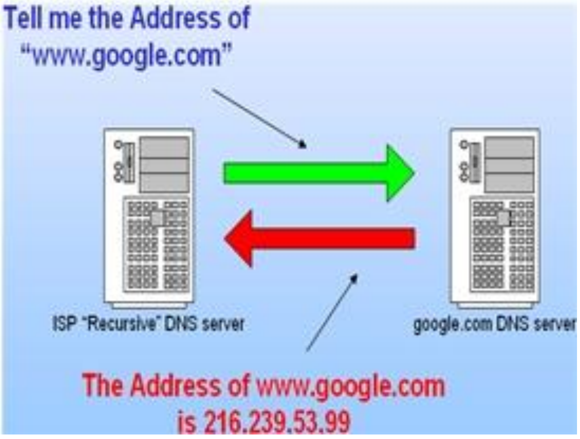


Fig 6: Step 3 DNS Servers work

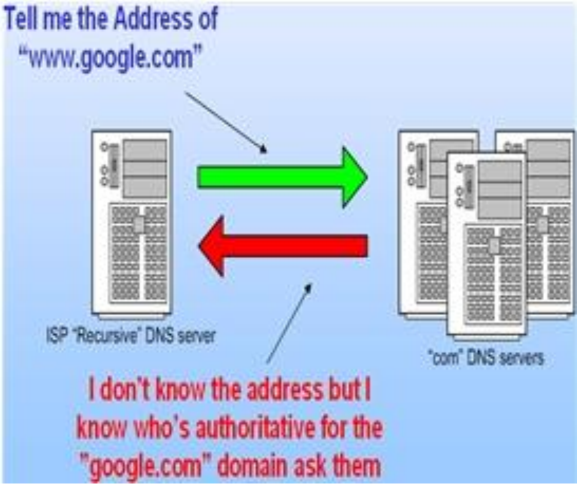

Tell me the Address of
"www.google.com"
ISP "Recursive" DNS server
"com" DNS servers
I don't know the address but I
know who's authoritative for the
"google.com" domain ask them

Fig 7: Step 4 DNS Servers work

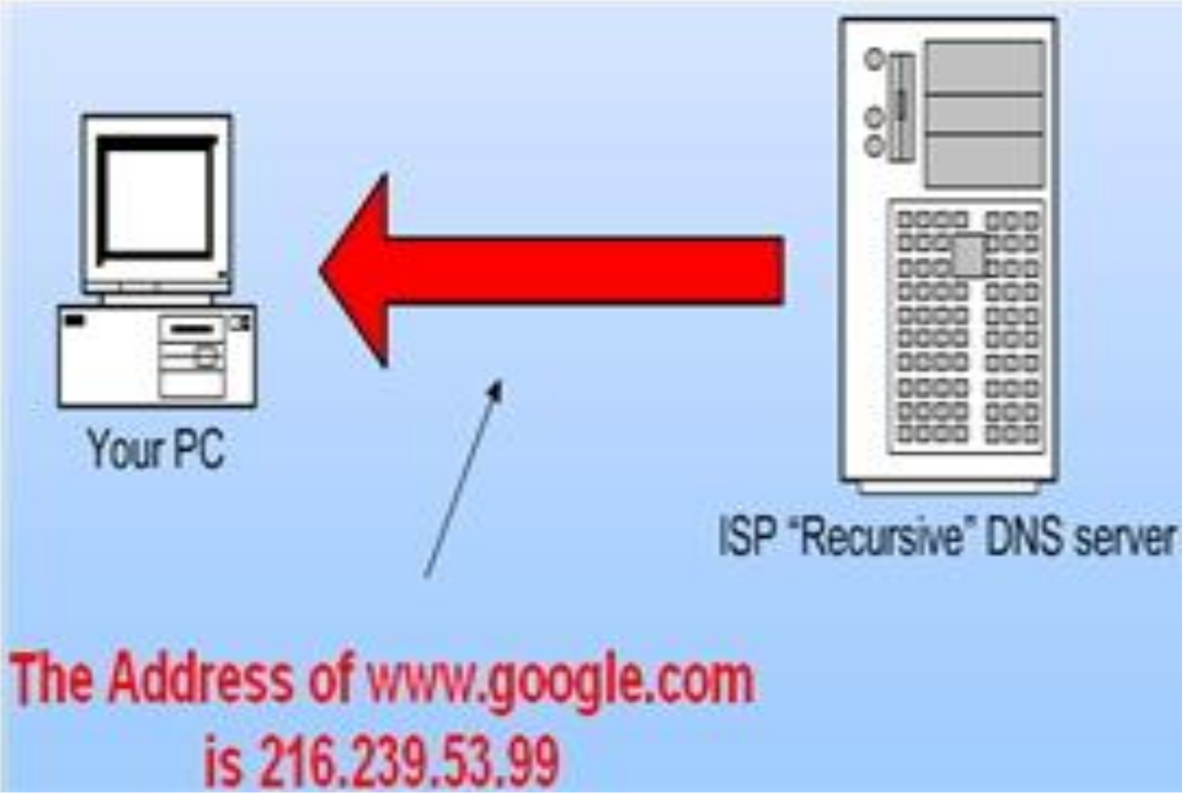


Fig 8: Step 5 DNS Servers work

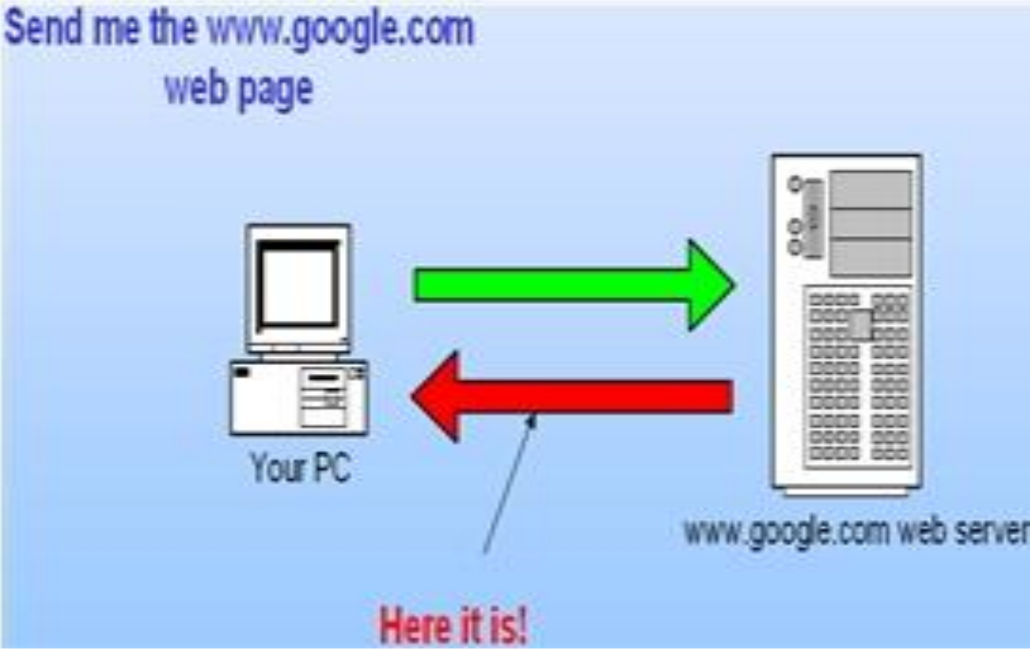


Fig 9: Step 6 DNS Servers work

- Within every top-level domain there is a huge list of 2nd level domains.
- For example, in the COM second-level domain, we've got:

- yahoo
- msn
- microsoft
- plus millions of others.

DNS naming structure Example: The DNS Naming Structure example is as follows:

How DNS Servers work?

Given below is the working of DNS on the web: You type http://www.google.com into your web browser and hit enter.

This involves various steps, which are as follows along with the diagrams:

Step 1: The computer(PC) sends a resolution request to its configured DNS Server, typically at your ISP.

Step 2: Your ISPs recursive name server starts by asking one of the root servers predefined in its “hints” file[3].

Step 3: Your ISPs recursive name server then asks one of the “com” name servers as directed.

Step 4: Your ISPs recursive name server then asks one of the “google.com” name servers as directed.

Step 5: ISP DNS server then send the answer back to your PC[5]. The DNS server will “remember” the answer for a period of time

Step 6: Your PC can then make the actual HTTP request to the web server.

III. DNS ORGANIZATIONS

The various points about DNS organisations are as follows:

- Internet Network Information Center(INIC) - This is US government owned.
- INTERNIC formerly handles all domain name registration
    - www.internic.net
- Network Solutions, a private company, processed the registrations.
- Several companies can register domains on their website.
- ICANN - The Internet Corporation for Assigned Names and Numbers, is a non-profit corporation that is designated by the U.S. Government to coordinate certain Internet technical functions, including the management of Internet domain name system

ICANN has the website - http://www.icann.org

IV CO-LOCATED DNS

Colocation is the placement of several entities at several locations. Thus, placement of several DNS at various locations is called Colocated DNS[4].

The example of the co-located DNS is as follows:

- In the online railway booking system, the user booking from north region will be directed to the dns in the northern zone.
- In the same way, the user booking from south region will be directed to the dns in the southern zone.
- The users from one region very rarely book tickets from other region.

- Thus, there is the need of the co-located DNS.

V. REFERENCES

[1] Christian Seifert, Ian Welch, Peter Komisarczuk and Chiraag Uday Aval, Barbara Endicott-Popovsky, “Identification of Malicious Web Pages Through Analysis of Underlying DNS and Web Server Relationships”, IEEE, 2008

[2] Steven Cheung and Karl N. Levitt,“A Formal-Specication Based Approach for Protecting the Domain Name System”,IEEE,2000

[3] Hiroshi Yokota, Shigetomo Kimura and Yoshihiko Ebihara, “A Proposal of DNS-Based Adaptive Load Balancing Method for Mirror Server Systems and Its Implementation”,IEEE, 2004

[4] Chih-Chiang Yang, Chien Chen and Jing-Ying Chen, “Random Early Detection Web Servers for Dynamic Load Balancing”, IEEE, 2009

[5] Fanglu Guo Jiawu Chen Tzi-cker Chiueh, “Spoof Detection for Preventing DoS Attacks against DNS Servers”, IEEE, 2006

[6] C.L. Schuba, and E.H. Spaord, “Addressing Weaknesses in the Domain Name System Protocol”, Technical Report, Department of Computer Sciences, Purdue University, 1994.

[7] W.Venema, TCP Wrapper: Net work Monitoring, Access Control, and Booby Traps." Proc. of the 3rd UNIX Security Symposium, September 1992.

[8] D. Danchev, “Dancho danchev‟s blog - mind streams of information security knowledge,” Available from http://ddanchev.blogspot.com/.

[9] Websense, Inc., “Blogs - security labs,” Available from http://securitylabs.websense.com/content/blogs.aspx.

[10] C. Seifert, R. Steenson, T. Holz, Y. Bing, and M. A. Davis, “Know your enemy: Malicious web servers.” The Honeynet Project, 2007, Available from http://www.honeynet.org/papers/mws/.

[11] Y.-M. Wang, D. Beck, X. Jiang, R. Roussev, C. Verbowski, S. Chen,

and S. King, "Automated web patrol with strider honeymonkeys: Finding web sites that exploit browser vulnerabilities," in 13th Annual Network and Distributed System Security Symposium. San Diego: Internet Society, 2006.

[12] A. Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy, "A crawlerbased study of spyware on the web," in 13th Annual Network and Distributed System Security Symposium. San Diego: The Internet Society, 2006.