International Journal of Computer Networks and Communications Security

VOL. 2, NO. 5, MAY 2014, 158–167
Available online at: www.ijcncs.org
ISSN 2308-9830

A Comparative Analysis on Existing DNS Performance Measurement Mechanisms

Ejaz Ahmad[1] and Kashif Sarwar[2]

[1] Ericsson Ltd, Middlesex University, London, United Kingdom

[2] Cyber Age Ltd, London, United Kingdom

E-mail: [1]ejazahmad9@gmail.com, [2]kashif_sarwar78@hotmail.com

ABSTRACT

DNS maps the complex IP addresses, making it crucial for internet communication for users and applications. DNS, an integral component of internet, is faced with many challenges. Enormous data growth and inherent security weakness demands continuous monitoring and performance measurement of DNS traffic. DNSSEC can improve security at the cost of DNS performance. This tradeoff needs to be evaluated before actual implementation. DNS performance measurement is critical for this evaluation. IPv6 will increase load on DNS exponentially, resulting in greater need for DNS performance evaluation. Despite the critical need for DNS performance measurement, very little research has happened on DNS performance measurement. Most of this little research has been done on client and authoritative layers of DNS. The most vulnerable and functionally important Caching layer performance measurement is hugely under researched. There are some software and hardware techniques available for DNS performance measurement. The software techniques provide burst of unrealistic data for limited time, restricting the scope of performance measurement and evaluation. Hardware data generation systems can be both expensive and inflexible. There is a need for more realistic DNS data traffic which can be used for flexible and cost effective performance measurement over a longer period for thorough evaluation.

Keywords: *DNS Performance Measurement, DNS Traffic generation, DNS Security, DNS Challenges, DNS Growth.*

1 INTRODUCTION

Domain Name System (DNS) corresponds to a distributed name resolution database which is resolvable universally. It provides user friendly interface without remembering complex IP addresses while browsing the internet. From communication point of view, functionality of almost every modern application relies on this protocol. Reza Curtmola (Curtmola, Sorbo and Ateniese, 2005) states that the role of DNS is vital, as it is involved in virtually every Internet transaction.

To users, it hides the complex mapping of IP addresses to domain names and clients are not required to remember difficult IP addresses for using internet. For instance, it is very easy to remember google.com compared to 74.125.227.67. With the evolution of IPV6, it has become even more difficult to remember 128 bit long IP address. Hierarchical nature of DNS helps to organize and access computer resources in a structural manner.

Modern computer applications are mainly reliant on DNS resolution for their basic functionality. For example, Microsoft Active directory mainly relies on DNS to perform its functions. DNS makes communication more robust. It is clear from Figure 1 that communication via DNS provides more flexibility and portability. Most importantly, DNS system provides interface for applications to communicate without relying on IP addresses. DNS facilitates continuous communication even if IP address of application is changed; providing seamless communication between applications.

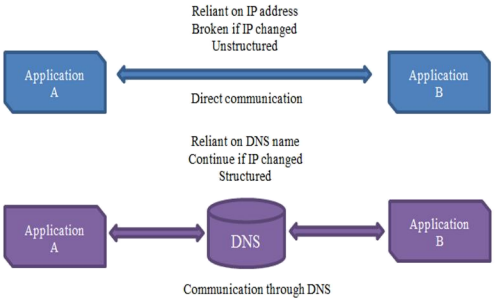

Fig. 1. Communication via DNS

DNS protocol will remain the focal point for all IP based communication due to its flexibility and adaptation and will act as a binding force for users and applications (Verisign, 2013).This crucial component of internet communication has its challenges. The security challenges and the effect on DNS performance has been explained in next section 2. This impact need to be quantified before security can be enhanced to e.g. DNSSEC. The exponential growth in IP addressed nodes and the huge DNS traffic resulting from it needs to be tested on DNS servers for DNS performance evaluation before being directed to the actual production environment. Section 3 details the existing research on DNS performance measurement at all three layers. There is extremely limited research done on caching layer which is the most vulnerable and functionally important. Majority of the DNS performance measurement is done on client and authoritative layers of DNS. Section 4 describes the available software and hardware systems for DNS performance measurement in the industry. This section explains the limitations of the existing systems. Section 5 concludes this research paper. Section 6 suggests the future work required on the performance measurement of DNS.

2 CURRENT DNS CHALLENGES

DNS performance measurement and trend analysis is one of the biggest challenges for today's cyber community as functionality of whole internet is dependent on this fundamental component (Casalicchio, Caselli and Coletta, 2013) . For a networked organization, any adverse issue with DNS would immediately impact inbound and outbound services, jeopardizing goodwill and revenue significantly. DNS monitoring is critical. Researchers and internet service providers continuously monitor DNS traffic for identifying anomalies, measuring performance, and generating usage statistics (Deri et al., 2012) .

Continuous Review and Optimization of DNS Performance is essential to mitigate risks to the domain name infrastructure. The Current high profile DDoS DNS attacks on major key players have underlined the importance of hardening the DNS infrastructure. Having sophisticated DNS performance measurement mechanism in place will prove to be effective tool to measure the robustness of underlying platform and providing proactive protection (Verisign, 2013).

DNS protocol is faced with multiple challenges. Enormous data growth and inherited security weakness has weakened the reliability of this protocol. Online shift of business and social activities has resulted into exponential growth in DNS traffic and there is absence of any built-in response authentication mechanism. To support this growth, underlying core technologies like Domain Names Service must be capable enough to accommodate this expansion. The main challenges faced by DNS are Security, DNSSEC, growth in domain names and IPV6 launch. We will discuss these challenges in subsequent sections.

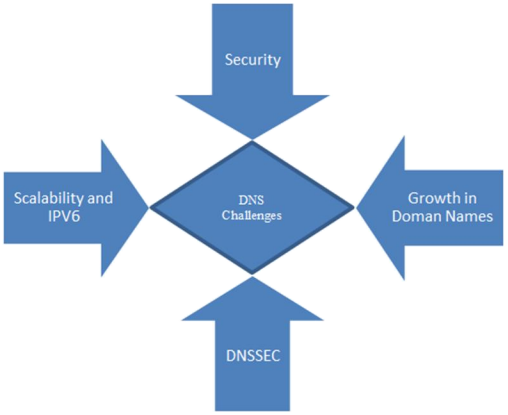

Fig. 2. Current DNS challenges

2.1 Security

With the discovery of inherited weaknesses in DNS, cyber community is growing more skeptical about the integrity of DNS. The whole internet can be brought to knees by attacking DNS as mentioned by the Kaminsky in his cache poisoning experiment (Kaminsky, 2008). This critical vulnerability of DNS protocol concerns the reliability of this protocol and security of internet as a whole. This critical flaw in the DNS protocol can be exploited; redirecting the internet traffic to illegitimate servers by poisoning the cache of domain name server.

Ever-increasing DNS attacks pose new challenges to the security practitioners. Sophisticated DNS attacks like Distributed Denial of Service (DDoS), man in the middle and other

complex and sophisticated DNS spoofing attacks force companies to engage resources to protect the DNS infrastructure by increasing cyber intelligence capabilities. It also requires careful DNS performance testing mechanism to optimize deployment to mitigate such attacks.

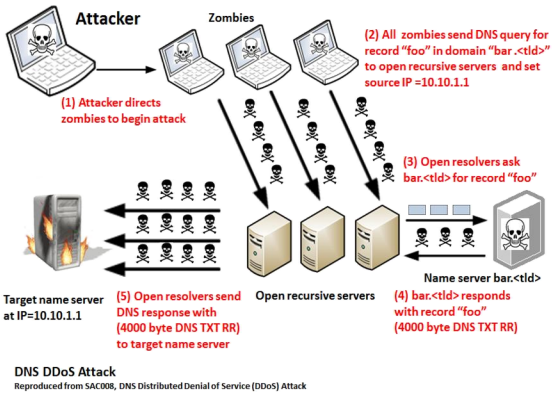

Fig. 3. DNS DDoS Attack

Inherited weak security mechanisms put DNS as a prime target to attack organizations and internet. This leads internet community to implement mitigation steps like DNSSEC across the end to end infrastructure. DNSSEC will provide a strong countermeasure to poisoning as well as other attacks against the DNS.(Trostle, Van Besien and Pujari, 2010)

2.2 DNSSEC

Moving towards DNSSEC arena, the performance measurement has become more important as combining this complex feature with existing DNS protocol implementations increases the load on applications; hence impacting the performance of platform. Domain name servers will see a growth in the size of its cache as well as see bandwidth impacts; it will also see a growth in CPU time dedicated to DNS operations (NIST, 2009). Experiment shows that using DNSSEC resulted in a 25% drop in performance (queries per second) for ANS and 38% for BIND. The DNSSEC databases consumed 20 times more space on the hard drives; bandwidth usage was 10 times bigger; and 4 times more memory was required with BIND.(Guillard, 2006)

Majority of DNS platform processing power would be utilized in processing crypto graphical nature of DNSSEC; requiring the upgradation of underlining platforms. In this scenario DNS performance measurement environment is vital to continuously measure, monitor and upgrade the capabilities of existing DNS infrastructure.

2.3 Growth in Domain Name

In recent years, enormous growth of DNS queries on the internet has come into spotlight; Internet Grows to More Than 252 Million Domain Names across all Top- Level Domains (TLDs) in the fourth Quarter of 2012, a report published by VeriSign, the trusted provider of Internet infrastructure services for the networked world(Verisign, 2013; Verisign, 2012). It also stated an increase of 6.1 million domain names over the third quarter of 2012, domain registrations have grown by 26.6 million or 11.8 percent, year over year. The base of Country Code Top-Level Domains (ccTLDs) increased to 110.2 million domain names, a 5 percent increase quarter over quarter, and a 21.6 percent increase year over year in the base. The following figure provides graphical representation for growth in top TLDs by zone size.

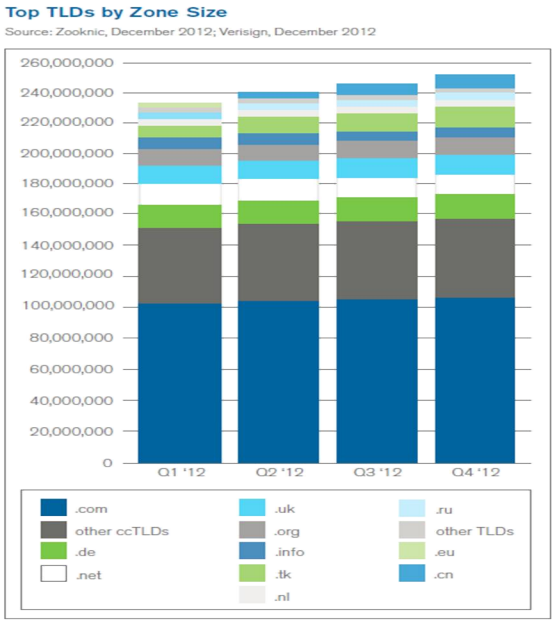

Fig. 4. Top TLDs by zone size

More than 50 billion devices will be connected by 2020, revealed in a white paper by Ericsson, a global Telecom provider (Ericsson Limited, February 2011). The paper also states that everything that can benefit from a connection will have one. According to Ericsson, there is a profound change in the way people, business and society interact. As a people we are already online. The next step is to get things and places online. This would put a huge load on Domain Name System which would be the key service to connect human with things and places. To meet this demand, existing performance of DNS platforms needs to be measured accurately. It is also required

to do performance tests of various DNS platforms to select best suited to meet the forecasted demand.

2.4 Scalability and IPV6

IPv6 overcomes the shortcomings of IPv4 by providing enough scalability to even facilitate billions of IP addresses per user. However, IPv6 format is not easy to remember. For example, it is unlikely someone can easily memorize and type 2001:0db6:75a3:0000: 4375:8a2e:2370:7435 on browser. Devices need to be globally accessible and thus need to have global names (Davies, June 2012). The role of DNS has become more vital here. IPv6 is designed to solve shortcoming of IPv4 and supports a nearly unlimited number of devices that can be directly connected to the Internet (Microsoft, 2013).

By delivering a 128-bit address format, IPv6 delivers sufficient capacity for an estimated 340 undecillion -- enough to award one to every grain of sand on the planet(Suomela, 2001).The following graph shows the percentage of networks (ASs) that announce an IPv6 prefix for a specified list of regional Internet registry (RIR) and countries(UK&USA).

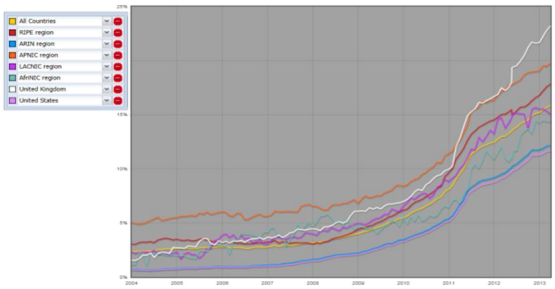

Fig. 5. Percentage of networks that announced IPv6 for specified RIR

IPV6 addresses are too complex to remember; IPV6 facilitates devices to be accessed globally using global names. DNS traffic will increase dramatically with IPV6 resulting in increased load and memory requirement (Nominum, 2012). DNS is a must in IPv6 network. In IPV6 world, all nodes including users, servers, routers, switches and firewall use DNS names to communicate.

3 PERFORMANCE MEASUREMENT

Measuring the performance of Domain Name Service platform is significant to the continuity of business and critical services of an organization. By evaluating the capability of existing platform by sophisticated techniques helps in deployment of suitable DNS infrastructure which can ensure the continuity of services in a business. For example, Verisign's average daily Domain Name System (DNS) query load during the third quarter of 2012 was 67 billion with a peak of 102 billion. Compared to the previous quarter, the daily average decreased 1.3 percent and the peak increased 14.1 percent (Verisign, DECEMBER 2012). To fulfill this high demand, Verisign DNS system needs to be measured and tuned to meet these demands.

Base lining the capability of existing Domain Name Service platform by performance measurement techniques is also required for selection of fit for purpose platform for an organization. For instance, by knowing the existing capability and current traffic volume combined with the projected forecast will ensure the deployment of appropriate system to meet the future demands. It will also provide a timescale for upgrades and advancement. Especially in service provision environment, the additional load on infrastructure needs to be analyzed when hosting new services or bring new customers. In case of load exceeding the current capacity, additional DNS servers can be deployed. It also helps to cope with new DNS vulnerabilities challenges and advancement by providing enough headroom in case of attacks.

To restore existing DNS protocol implementation which inheritably lacks the data security features, vendors are investing time and efforts to come up with a solution which can deal with these challenges occurring from technological advancement. This leads DNS developers and vendors to come up with new software releases, patches and upgraded versions. This forces the whole DNS community to continuously and frequently upgrade their DNS infrastructure by testing and measurement of existing platform so that their existing solutions are not vulnerable to sophisticated cyber-attacks.

Due to high vulnerability associated with DNS protocol, the frequency of DNS Vulnerability Disclosure is higher. With every software upgrade or patches to existing code, the reliability and capability of updated code is not known. Vendor advisory committee recommends upgrading to latest release but stability and capacity of new code must be established. If not tested carefully, new code could hugely impact the entire production environment. Therefore a comprehensive testing mechanism is vital to provide stable services. This helps to build the organization’s confidence in new DNS environment; comparing its reliability and accuracy by pre-deployment testing. Similarly, in case of hardware upgrades, it is equally important for an organization to find out the capability of new

platform using performance measurement techniques.

3.1 Performance measurement existing literature /background work

The main components of DNS platform consists of server hardware, operation system and DNS application that run on this server. Some vendors offer appliance solution consisting of the combination of hardware with custom built operating system and application. The parameters that interest organizations for DNS performance measurement are CPU usage, memory utilization, successful queries, failed queries, NX domain queries, cache contents etc. These parameters are normally collected by any monitoring tools.

The following diagram highlights the DNS functional model in general.

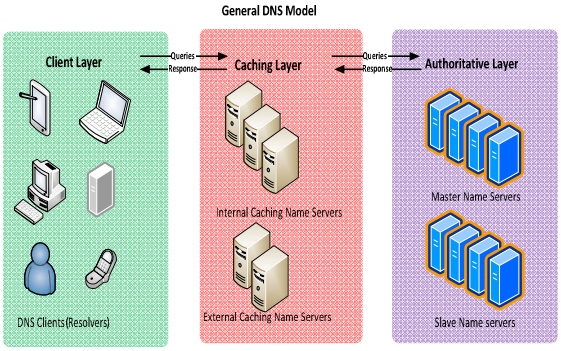

Fig. 6. General DNS Model

Generally, DNS functional architecture consists of 3 layers. These layers or DNS roles can be combined depending on requirement.

1: Client side that mainly consists of resolvers sending DNS queries.

2: Caching layer is mainly responsible for resolving queries and responding back to resolvers with final answer

3: Authoritative layer provides reference to specific DNS server responsible for maintaining the authoritative record for particular DNS queries.

Despite the most critical role of DNS in modern day internet, there is hardly any full scale, direct research on DNS performance measurement and development of testing environment for DNS monitoring. There are few limited scale performance measurement studies focusing on client side or authoritative servers (some of them are mentioned in next section). Despite the fact that caching DNS servers are the most critical in terms of utilization and vulnerabilities; there is little known research on this layer of name servers.

Diversity in DNS performance Measures (Liston, Srinivasan and Zegura, 2002) is a client side study providing the operations of the client side DNS system from the various locations on the internet to determine which measures vary based on location and which measures remain relatively constant. But this does not specify the actual DNS Server performance measurement. In another study 'On the effectiveness of DNS-based server selection' (Shaikh, Tewari and Agrawal, 2001) discuss the negative effects of reducing the cache lifetimes of DNS information and the implicit assumption that client name servers are indicative of actual client location and performance. This study is also silent about the modern DNS measurement strategies.

An interesting research paper "Towards a Passive DNS Monitoring System" (Deri et al., 2012) provides Italy TLD DNS traffic analysis to understand the trends and interests of a country by analyzing queries to TLD domain servers. It covers the design and implementation of a passive DNS monitoring system whose goal is to understand trends, characterize economical relationships and also tracks suspicious activities by collecting information from the .it country code (Italy) Top Level Domain (TLD) which is deployed on .it authoritative name servers. However this research focuses on traffic analysis rather than DNS performance measurement. Moreover the research field is Italy .it top level domain TLD and does not discuss general DNS performance. The research emphasizes on DNS authoritative server and not applicable to cache DNS server which forwards queries to TLDs; particularly current DNS traffic growth issues and underlying performance measurement mechanism.

Another client side study (Marchal and Engel, 2012) presented a method to identify and compare domain names activities leveraging features that are extracted from DNS response packets collected at resolver. Another study using the traditional tools shows the impact of DNSSEC implementation on a typical large ISP's DNS platform (Guillard, 2006) used an authoritative server running BIND and ANS and a client running Queryperf proved that performance drop should be expected when using DNSSEC. The same fact has been highlighted in the study (Curtmola, Sorbo and Ateniese, 2005) showing the adding security will lower DNS performance using BIND 9 and Queryperf.

About scalability of DNS, (Jaeyeon, et all., 2002) discussed the factors contributing to the scalability of DNS (hierarchal design and administratively delegated name spaces) and had run some limited volume test to prove it. He used software

application tcpdpriv, a utility based on tcpdump packet capture library. In terms of root server effectiveness, (Danzig, et al.,1992) presented measurements of DNS traffic at a root name server. Their main conclusion was that the majority of DNS traffic is caused by bugs and miss-configuration. In an article titled CoDNS: Improving DNS Performance and Reliability via Cooperative Lookups, (KyoungSoo et all., 2004) discussed the client side service to improve the client side lookup efficiency. They developed a lightweight name lookup service, CoDNS that uses peers at remote sites to provide cooperative lookups during failures. This however focuses on client layer.

4 EXISTING DNS PERFORMANCE MEASUREMENT TECHNIQUES AVAILABLE TO INDUSTRY

The query throughput of a DNS server is defined as how many queries per second a DNS server is capable of handling. Measuring the volume of queries a server can handle in a customized environment is very important to the organization as this allows forecasting the scalability of the solution. This would help to find out the existing headroom and time estimation of future run out period to plan more capacity. Next section is going to highlight various techniques in use by industry to determine the performance and behavior of name servers.

4.1 DNS performance testing Software tools

In industry as well as in research, dnsperf, resperf and queryperf are widely used for DNS performance testing for years. Nominum (www.nominum.com) developed two software programs- dnsperf and resperf. Dnsperf is an authoritative-server-specific Domain Name Service (DNS) performance testing tool which can be used for catching server performance in a closed laboratory environment. However preferred program for measuring the resolution performance of caching DNS server is resperf. These software based performance testing tools run on client machine and send queries to DNS server under test preferably on a directly connected Ethernet segment (Nominum, 2013).

Resperf, unlike dnsperf, sends DNS queries at a controlled, steadily increasing rate. By default, resperf sends traffic for 60 seconds, linearly increasing the amount of traffic from zero to 100,000 qps-queries per second (Nominum, 2013). Query input file containing DNS requests is required to run the test. The software run on command line for a short time and display output on a command line or directing the command output to a file that creates an HTML report; with resulting parameters. The software program can be installed on the same machine which is under test. However preferred approach is to run this program on a separate server dedicated for generating test traffic.

According to Nominum, maximum throughput of underlying platform is determined by the highest response rate on the plot OR the response rate at the point where a significant number of queries begin to be dropped. By default, the maximum throughput is the highest point on the response rate plot, without regard to the number of queries dropped or failing at that point. Test runs for couple of minute and resperf takes 100 seconds at most, comprised of 60 seconds of traffic ramp-up followed by 40 seconds of waiting for responses.

The following example and graph show sample output from the resperf command (Nominum, 2013):

DNS Resolution Performance Testing Tool
Nominum Version 2.0.0.0.d
[Status] Command line: resperf -p 12345 -d in
[Status] Sending
[Status] Fell behind by 1039 queries, ending test at 39331 qps
[Status] Waiting for more responses
[Status] Testing complete
Statistics:
Queries sent: 463036
Queries completed: 463036
Queries lost: 0
Run time (s): 100.000000
Maximum throughput: 36250.000000 qps
Lost at that point: 0.00%

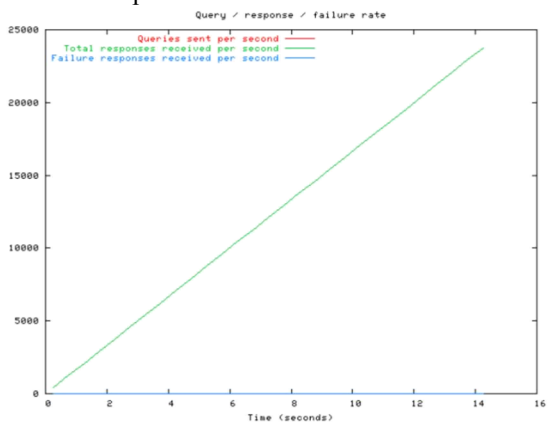

Fig. 7. Query/Response/Failure Rate Plot

Queryperf is a DNS server query performance tool which is included in the well-known DNS open source BIND distribution by ISC

(https://www.isc.org).It is very similar to dnsperf/resperf and widely used for performance measurement of the authoritative and caching DNS servers. "Queryperf" is commercial based performance tool being used widely in the industry. This query performance testing tool is bundled within the BIND 9 distribution by ISC.

Queryperf provides top-end performance of a test server by determining the DNS queries processing power of underlying server. For testing execution, DNS data input file is required similar to Nominum testing tool. This file contains domain name and type of query look up and can be built manually. This tool can be used for both authoritative and catching servers. Various command switches can be used to mention parameters like time, input file, server and ports etc. The following is the sample output (Liu, 2003).

DNS Query Performance Testing Tool
Version: $Id: ch05.xml,v 1.3 2002/10/16 20:08:21 becki Exp $
[Status] Processing input data
[Status] Sending queries
[Status] Testing complete
Statistics:
Parse input file: multiple times
Run time limit: 60 seconds
Ran through file: 0 times
Queries sent: 265935 queries
Queries completed: 265935 queries
Queries lost: 0 queries
Percentage completed: 100.00%
Percentage lost: 0.00%
Started at: Mon May 13 16:26:28 2002
Finished at: Mon May 13 16:27:28 2002
Ran for: 60.458815 seconds
Queries per second: 4398.614164 qps

The above mentioned software tools are more practical and have been used for many years by the internet community for performance measurement. However there are certain limitations of these tools. In terms of output, they provide only pre-define fixed parameters and are not very flexible. For example after running tests resperf displays fixed parameters like queries sent, completed, lost, response, failure, latency and Maximum throughput etc. The output cannot be customized to provide additional parameters critical for an organization like DNS queries per second, server memory utilization, CPU usage, Cache contents, Cache hit ratio, recursive clients, response time, and DNS record types (MX, NS, SOA, SRV, PTR, AAAA, A, CNAME, NXDOMAIN etc.)

For executions, the software requires pre-populated DNS data files as a query input file. Sample query data file is provided by Nominum for dnsperf and resperf but it can also be built by logging DNS server queries from production servers. However there is finite number of DNS record set in this file and tests cannot be run for ongoing basis and stops after couple of minutes. Also it is required to select different domain names in query input file otherwise name server would cache the answers and representative measurement of performance wouldn't be accurate.

To avoid data file size limitations, a script can be used for run tests continuously but this approach does not provide actual presentation of production environment. Moreover DNS record sets are already cached and use the repeated data file which jeopardizes the test results. Therefore these software cannot provide always on test beds. Moreover, it is not easy to produce large volume of constant queries and requires a dedicated machine with this software installed on it, to generate streams. In some scenarios, it may require several machines to produce enough simultaneous query streams to create a high enough load that's equivalent to real queries.

The following diagram illustrating two machines loaded with queryperf software testing tools and use input query file to load test target name server.

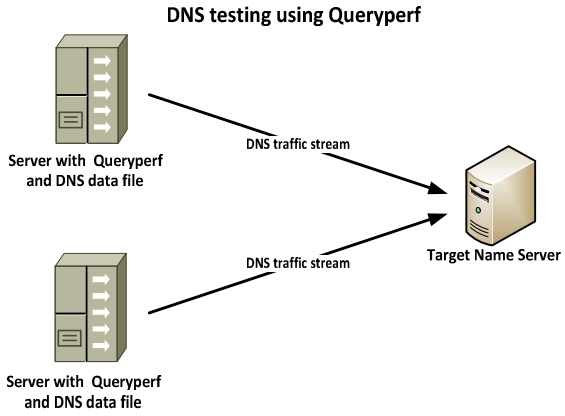

Fig. 8. DNS testing using Queryperf

This software simulates artificial environment and the queries generated are not a true representation of real time behavior in terms of frequency, type of domains and bandwidth etc. Moreover, this option also requires installation of extra hardware for installation of testing software and generation of DNS traffic.

4.2 Traffic Generators Hardware Appliances

Traffic Generator appliances are hardware equipment used for traffic simulation. These appliances are expensive and their prices vary with

the requirement of bandwidth. Traffic generators can potentially be used for simulating DNS traffic but offer less flexibility. Moreover, the test environment does not represent real scenarios.

Other issues are extra hardware required, installation set up and static nature of testing, and less flexibility. These are also not built specifically for DNS protocols. Fox example, Spirent Communications, SmartBits tests, simulates, analyzes, troubleshoots, develops, and certifies the network infrastructure. This general purpose appliance helps from initial design to ongoing testing of the final network, SmartBits (spirent, 2013). Another example of traffic generation appliance called Packetjet is a packet generator engine and is used for packet generation and injection for testing network intrusion detection systems, firewalls, IP stacks etc. Packetjet can also craft ARP, DNS, Ethernet, ICMP, IGMP, IP, OSPF, RIP, TCP and UDP packets (Rsignia, 2013).

LANforge FIRE generates and receives various network protocols. It is used to create load on a network under test (Candela Technologies, 2013). It can generate load against web servers, VOIP gateways, firewalls, load-balancers and many other network components. Candela states that LANforge supports Layer 4 DNS .It is used and reported by most Layer 4 traffic types.

These hardware appliances are used to generate load against network components like web servers, VOIP gateways, firewalls etc. but not specifically designed for DNS traffic. For DNS it does not provide granularity, flexibility, intuitiveness and real-life traffic patterns. These appliances are expensive and normally require extra cost with licensing for every feature. The traffic generated is static in nature and requires manual input as domain names and not actually mirroring of real time traffic. Particularly for DNS testing, these appliances are not widely used in the industry. They are very expensive and also have limited bandwidth like 1Gigabit, 2 Gigabit etc. In some extreme scenarios, they are not scalable enough to generate enormous amount of queries and require multiple traffic generators to emulate large volume of DNS queries.

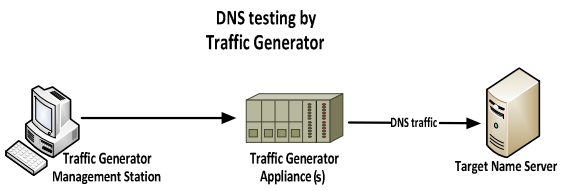

Fig. 9. DNS testing by Traffic Generator

4.3 General Purpose Testing Software

There are widely available general purposed software tools available for measuring the TCP/UDP traffic which can measure different protocol like World Wide Web (www), File transfer protocol (FTP) servers. Some of these can also be used for DNS protocol but are not specifically designed for this protocol and lacks many vital features. Most importantly, these tools are good to testing the functionality and accuracy of name server rather than load testing or performance measurement testing. Most of them are simple, free, open source software program developed by volunteers to perform basic network testing. As DNS is based on UDP protocol so these tools can be used for limited testing of DNS service at small scale.

Nemesis is a command-line network packet crafting and injection utility for UNIX-like and Windows systems. This open source freeware applications is used for general testing of Network Intrusion Detection Systems, firewalls, IP stacks and others. Nemesis can natively craft and inject ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP and UDP packets (Nathan,J)

Another example is application named Mausezahn. This is a free traffic generator written in C which allows crafting different packets. It is mainly used to test VoIP or multicast networks but also for security audits to check whether systems are hardened enough for specific attacks. The functionality can be scaled to DNS. However, this application has a very limited capability for this protocol, Mausezahn (Herbert, 2009). Another tool packeth is a GUI and CLI packet generator tool for Ethernet which creates and sends any Ethernet packet like UDP, TCP, ICMP, ICMPv6, IGMP and others(Jemec, 2013).

However these tools are not viable for large scale testing. They are only useful for generating limited amount of DNS traffic for verification of basic DNS features but not tailored to meet the specific requirements of the Domain Name Server protocol and do not offer flexibility and scalability to handle large number of queries. The freeware applications available do not offer flexibility and cannot be used for creating enormous amount of DNS queries.

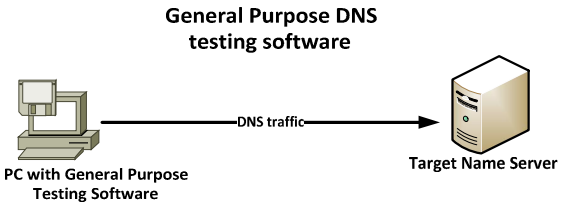

Fig. 10. General Purpose DNS testing software

5 CONCLUSION

DNS maps the complex IP addresses to domain names and provide seamless communication between applications. Modern day internet is heavily reliant on DNS, which carries inherent vulnerabilities. The main challenges faced by DNS are security, DNSSEC, growth in domain names and IPV6 launch. DDoS, Man in the middle and other sophisticated DNS spoofing attacks mitigation require careful DNS performance testing mechanism. DNSSEC combined with DNS protocol impacts the performance by increased CPU time dedicated to DNS operations, more space consumption on hard drive, greater bandwidth usage and more memory space required. Internet has experienced exponential growth in last decades. DNS traffic will increase dramatically with IPV6, resulting in increased load and memory requirement. To meet the challenges faced by DNS, existing performance of the DNS platforms need to be measured accurately.

Evaluating the capability of existing platforms by sophisticated techniques helps in deployment of suitable DNS infrastructure. By knowing the existing capability and current traffic volume combined with the projected forecast will ensure the deployment of appropriate system to meet the future demands. Most of the little research on DNS performance measurement has taken place at client and authoritative layers, leaving behind caching layer under researched despite the fact that caching DNS servers are most critical in terms of utilization and vulnerabilities. Dnsperf, resperf and queryperf are well known performance testing software tools in use for years. The output of these test programs is linear and constrained not including important DNS parameters like successful/failed queries, DNS records types, memory utilization, CPU usage, cache contents, cache hit ratio, recursive clients and response time etc. Traffic generator hardware appliances are used to simulate DNS traffic. This hardware is very inflexible and expensive, offering static testing. These traffic generators are not built specifically for DNS protocols resulting in non-real representation for real scenarios. There are some open source general testing applications which can only be used for DNS performance measurement at a small scale.

Performance measurement of DNS needs to be done on realistic traffic data leading to scruples evaluation. Continuous monitoring over a long period enables to pick abrupt changes in the pattern resulting from malicious attack. Any new monitoring scheme should be cost effective and non- intrusive to the natural behavior of the network. There is a need for flexible DNS performance measurement scheme resulting into customizable parameters.

6 FUTURE WORKS

There is a huge gap for research on performance measurement on Caching layer of DNS. DNS performance measurement schemes need to be devised which are flexible, analyze realistic DNS traffic, large scale, cost competitive, always on and non-intrusive. Industry needs a real time test bed parallel to production network for patches and upgrades evaluation, pre-deployment testing, attack mitigation processes, platform capability assessment, traffic forecasting and headroom for attacks (business continuity) and vulnerability assessment.

7 REFERENCES

[1] Cadela Technologies (2013) LANforge FIRE Stateful Network Traffic Generator. Available at: http://www.candelatech.com/datasheet_fire.php (Accessed: 4/27/2013 2013).

[2] Casalicchio, E., Caselli, M. and Coletta, A. (2013) "Measuring the global domain name system", Network, IEEE, vol. 27, no. 1, pp. 25-31.

[3] Curtmola, R., Sorbo, A. and Ateniese, G. (2005) "On the Performance and Analysis of DNS Security Extensions" in , eds. Y. Desmedt, H. Wang, Y. Mu and Y. Li, Springer Berlin Heidelberg, , pp. 288-303.

[4] Davies, J. (June 2012) Understanding IPv6, 3rd Edition edn, Microsoft Press, California 95472.

[5] Deri, L., Trombacchi, L.L., Martinelli, M. and Vannozzi, D. (2012) Towards a passive DNS monitoring system, ACM, Trento, Italy.

[6] Ericsson Limited (February 2011) More than 50 billion connected devices, www.ericsson.com.

[7] Guillard, A. (2006) "DNSSEC Operational Impact and Performance", 2006, vol. Proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI'06), no. IEEE.

[8] Jemec, M. (2013) packeth. Available at: http://packeth.sourceforge.net/packeth/Home.html (Accessed: 4/14/2013 2013).

[9] Kaminsky, D. (2008) "Catching up with Kaminsky", Network Security, vol. 2008, no. 9, pp. 4-7.

[10] Liston, R., Srinivasan, S. and Zegura, E. (2002) Diversity in DNS performance measures, ACM, Marseille, France.
[11] Liu, C. (2003) DNS and BIND Cookbook, 4th edn, O'REILLY, CA, USA.
[12] Marchal, S. and Engel, T. (2012) "Large Scale DNS Analysis" in , eds. R. Sadre, J. NovotnÃ½, P. ÄŒeleda, M. Waldburger and B. Stiller, Springer Berlin Heidelberg, , pp. 151-154.
[13] Microsoft (2013) Technologies and Solution-IPV6. Available at: http://technet.microsoft.com/en-gb/network/bb530961.aspx (Accessed: 2/18/2013 2013).
[14] Nathan, J. Nemesis: Packet injection tool suite. Available at: http://nemesis.sourceforge.net/ (Accessed: 4/14/2013 2013).
[15] NIST (2009) DNSSEC and its Impact on DNS Performance. Available at: http://www.dnsops.gov/dnssec-perform.html (Accessed: 2/11/2013 2013).
[16] Nominum (2013) Network Measurement Tools by Nominum. Available at: http://www.nominum.com/support/measurement-tools/ (Accessed: 4/5/2013 2013).
[17] Nominum (2012) IPV6- Beyond Business Continuity. Available at: http://learn.nominum.com/ipv6-webinar (Accessed: 2/18/2013 2013).
[18] Rsignia (2013) PacketJet - Multi Protocol Traffic Generator and Test Equipment. Available at: http://www.rsignia.com/index.php/cywarfius-solutions/packetjet.html (Accessed: 4/27/2013 2013).
[19] Shaikh, A., Tewari, R. and Agrawal, M. (2001) "On the effectiveness of DNS-based server selection", , pp. 1801 <last_page> 1810.
[20] spirent (2013) SmartBits. Available at: http://www.spirent.com/Products/Smartbits (Accessed: 4/27/2013 2013).
[21] Suomela, P. (2001) "Growing Into IPv6", Wireless Review, vol. 18, no. 23, pp. 10.
[22] Trostle, J., Van Besien, B. and Pujari, A. (2010) "2010 6th IEEE Workshop on Secure Network Protocols; Protecting against DNS cache poisoning attacks", , pp. 25 <last_page> 30.
[23] Verisign (DECEMBER 2012) THE DOMAIN NAME INDUSTRY BRIEF, Verisign, United States.
[24] Verisign (2013) THE DOMAIN NAME INDUSTRY BRIEF- VOLUME 10 - ISSUE 1 - APRIL 2013. Available at: http://www.verisigninc.com/assets/domain-name-brief-april2013.pdf (Accessed: 7/30/2013 2013).
[25] Verisign (2012) Internet Grows to More Than 246 Million Domain Names in the Third Quarter of 2012. Available at: https://investor.verisign.com/releasedetail.cfm?ReleaseID=728215 (Accessed: 02/10/2013 2013).

AUTHOR PROFILES:

Ejaz Ahmad heads a networking consultancy firm in the UK which provides network services to the leading telecommunication operators. He is a Cisco Certified internetwork expert (CCIE) in Security and a Check Point Certified Security Expert (CCSE). He is also a doctoral candidate at Middlesex University, London since 2010. He deployed two new Data centers for Kcom in 2013 as a lead Technical Design Authority (TDA) and helped in migration more than 500 remote sites. As an IP Design Architect at Ericsson he researched and pioneered a DNS performance mechanism which is flexible, real-time and cost effective, saving huge costs. As a Cisco IP research and design specialist at Arqiva Ltd, he supported high-tech projects like London underground digital signage and UK's switchover to digital television.

Kashif Sarwar received his MSc. in Computer Networks from Middlesex University in 2006. He has over 10 years of experience in Network/Systems research, design, implementation and network security. He has led team of Engineers in data center migration, designed and deployed ASRs in the network core at AlwaysOn (UK) in 2012. At H3G-UK in 2011, he decommissioned VPN concentrators and redesigned the entire security infrastructure with PIX and Checkpoint firewalls upgrades. He is actively involved in developing DNS performance measurement technique using real time traffic mirroring. His research interests include DNS performance evaluation, DNS security, e-government data center design and vehicular networks security.