Produce a technical plan for an "Irish" TRR

Tung-te Lin M.Sc.

A Dissertation

Presented to the University of Dublin, Trinity College

in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science (Future Networked System)

Supervisor: Stephen Farrell

11 2020

Declaration

I, the undersigned, declare that this work has not previously been submitted as an exercise for a degree at this, or any other University, and that unless otherwise stated, is my own work.

Tung-te Lin

October 19, 2020

Permission to Lend and/or Copy

I, the undersigned, agree that Trinity College Library may lend or copy this thesis upon request.

Tung-te Lin

October 19, 2020

Acknowledgments

...ACKNOWLEDGMENTS...

TUNG-TE LIN

University of Dublin, Trinity College
11 2020

Produce a technical plan for an "Irish" TRR

Tung-te Lin, Master of Science in Computer Science

University of Dublin, Trinity College, 2020

Supervisor: Stephen Farrell

...ABSTRACT...

Summary

...SUMMARY...

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Section 1.1

...

Chapter 2

The state of the art

2.1 The introduction of DNS

Before reading this paper, it is necessary to understand what DNS and TRR are, and what the problem would have in using traditional DNS and why TRR may resolve it.

DNS stands for Domain Name Server. The machines on networks have their own addresses to identify their locations. If users or machines do not have one's address, then they can not connect it or send packets to it.

There are two kinds of addresses, the first one is IP address, which is used for machines to recognize other machines. IP addresses can be IPv4 or IPv6, IPv4 consisted of 4 numbers(0 to 256) [8], for example 127.0.0.1 is IPv4. IPv6 consisted of 8 numbers(0000 to ffff) [9], for example 0000:0000:0000:0000:0000:0000:0000:0001 is IPv6. Numbers are easy to be processed by machines, therefore the addresses used by machine consist of numbers.

Contrarily, another kind of addresses is domain name. It consists of several words and is separated by dots, for example, www.tcd.ie is domain name. The words or strings are easy to be remembered by human, thus domain names are mainly used by human [10].

A machine needs a IP address in a network to be recognized by other machines, it can have a domain name to make people to remember it easily, but domain name is not compulsory in a networks. If people type a domain name on their web browser, their computers can translate the domain name into its IP address, then computers use the IP address to search the owner of this IP address in a network.

Hence, it is necessary that having a place to store IP addresses and domain names, moreover, the relations between domain names and IP addresses must be recorded, such as which domain name belongs to which IP address.

That place is so called Domain name server, which is DNS. When users type domain names, their computers use domain names to get correspond IP addresses in a DNS server [11].

Moreover, there are 2 kinds of DNS servers, which are recursive DNS resolver and authoritative DNS server. Recursive DNS resolvers do not save all the IP addresses and domain names that users need. If users query the domain names that the recursive DNS resolver does not know, then the recursive DNS resolver will inquire authoritative DNS servers about the IP address for the domain name. After that, the recursive resolver saves the domain name and its IP address in the cache, in case any users use this domain name in a short time, then the recursive resolver is able to reply its IP address immediately and not to inquire authoritative DNS servers again.

About authoritative DNS servers, they store IP addresses and domain names that users need, but users can not inquire them directly, because users have to utilize recursive DNS resolvers to inquire authoritative DNS servers to get correspond IP addresses.

Furthermore, authoritative DNS servers are hierarchical. The highest one is root server. A topper level authoritative DNS server can respond a address of a lower level authoritative DNS server to users for their inquiry, and that lower level authoritative DNS server may have the IP address what users need. In that case, a authoritative DNS server does not need to save entire IP addresses and domain names, the workload can be divided. The levels of authoritative DNS servers are shown in Fig. 2.1.

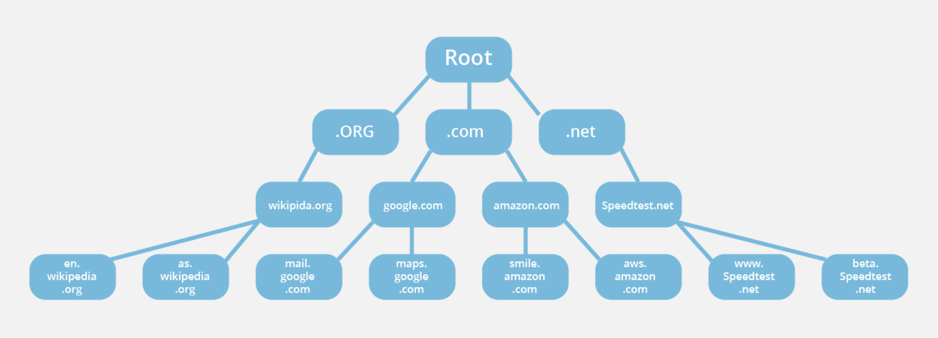
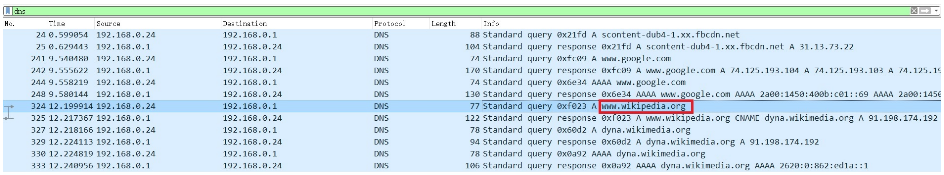


Figure 2.1: *The levels of authoritative DNS servers [4]*

2.2 The problem and solutions in using DNS

DNS servers make people more convenient, but it also has a problem. In using traditional DNS servers, the domain names that users query are not encrypted. Which means, if others get the packets from users, then they can understand what websites users browse or what applications users use.

Wireshark is the software for catching packets in a machine. This study utilized Wireshark to make a small test, when the researcher typed a domain name of a website on a web browser, then that domain name was displayed on Wireshark. The screenshot is shown in Fig. 2.2.



No.	Time	Source	Destination	Protocol	Length	Info
24	0.599054	192.168.0.24	192.168.0.1	DNS	88	Standard query 0x21fd A scontent-dub4-1.xx.fbcdn.net
25	0.629443	192.168.0.1	192.168.0.24	DNS	104	Standard query response 0x21fd A scontent-dub4-1.xx.fbcdn.net A 31.13.73.22
241	9.540480	192.168.0.24	192.168.0.1	DNS	74	Standard query 0xfc09 A www.google.com
242	9.555622	192.168.0.1	192.168.0.24	DNS	170	Standard query response 0xfc09 A www.google.com A 74.125.193.104 A 74.125.193.103 A 74.125.19
244	9.558219	192.168.0.24	192.168.0.1	DNS	74	Standard query 0x6e34 AAAA www.google.com
248	9.580144	192.168.0.1	192.168.0.24	DNS	130	Standard query response 0x6e34 AAAA www.google.com AAAA 2a00:1450:400b:c01::69 AAAA 2a00:1450
324	12.199914	192.168.0.24	192.168.0.1	DNS	77	Standard query 0xf023 A www.wikipedia.org
325	12.217367	192.168.0.1	192.168.0.24	DNS	122	Standard query response 0xf023 A www.wikipedia.org CNAME dyna.wikimedia.org A 91.198.174.192
327	12.218166	192.168.0.24	192.168.0.1	DNS	78	Standard query 0x60d2 A dyna.wikimedia.org
329	12.224113	192.168.0.1	192.168.0.24	DNS	94	Standard query response 0x60d2 A dyna.wikimedia.org A 91.198.174.192
330	12.224819	192.168.0.24	192.168.0.1	DNS	78	Standard query 0x0a92 AAAA dyna.wikimedia.org
333	12.240956	192.168.0.1	192.168.0.24	DNS	106	Standard query response 0x0a92 AAAA dyna.wikimedia.org AAAA 2620:0:862:ed1a::1

Figure 2.2: *The queried website is revealed in using a traditional DNS server*

Revealing the queried domain name can cause the severe privacy problem. People may not be willing to let others to find what websites they browse. Thus, some solutions were created.

DNSSEC

DOT

DOH

2.3 The introduction of TRR

...

2.4 The policy in Ireland

...

2.5 The demand of TRR in Ireland

...

Chapter 3

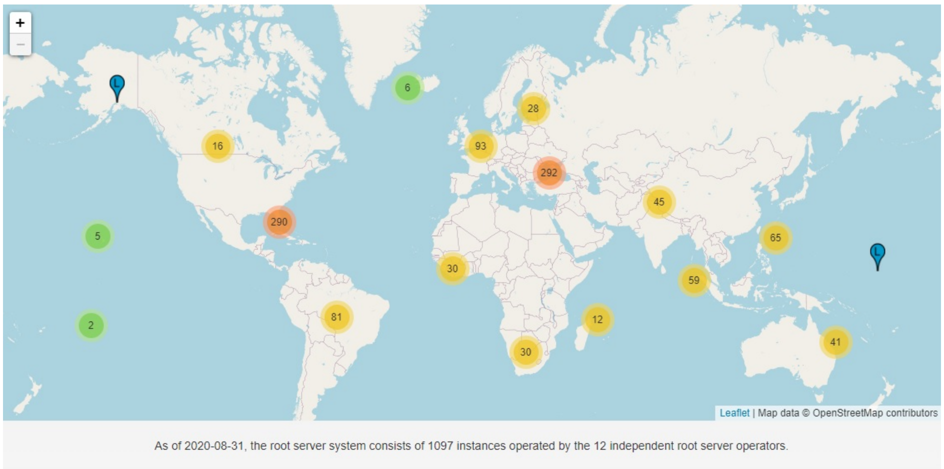
The DNS traffic in Ireland

The DNS traffic is an important consideration for building a DNS server. Irish TRR servers have to be capable to deal with the DNS traffic of national scale traffic in Ireland.

Before understanding the DNS traffic in Ireland, it is necessary to understand the root servers first.

Root servers are the highest level DNS servers [4], there are 1097 instances in the root server system on 31 August 2020. They are divided into 13 root server zones, each zone has a representative letter, which are A, B, C, D, E, F, G, H, I, J, K, L and M [12]. Those root server zones are managed by 12 organizations [1], which are Verisign(It manages 2 root server zones), USC-ISI, Cogent Communications, University of Maryland, NASA Ames Research Center, Internet Systems Consortium, Defense Information Systems Agency, U.S. Army Research Lab, Netnod, RIPE NCC, ICANN and WIDE Project. Therefore, those 12 organizations have the information about DNS traffic.

In the map from Root-servers.org, there are 8 root servers in Ireland, 5 servers are in Dublin and 3 servers are in Cork. As for organizations, 3 servers belong to



As of 2020-08-31, the root server system consists of 1097 instances operated by the 12 independent root server operators.

Figure 3.1: *The root servers in the world [1]*

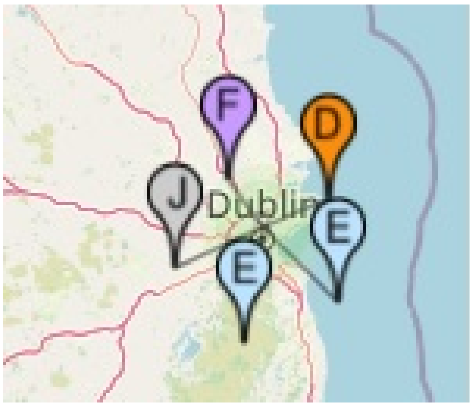


Figure 3.2: *The root servers in Dublin [1]*

E-root(E zone, it is managed by NASA Ames Research Center), 2 servers belong to F-root(F zone, it is managed by Internet Systems Consortium). K-root(RIPE NCC), D-root(University of Maryland), J-root(Verisign) have 1 server respectively [1].

The problem is the information those organizations provided on Internet is limited. There is no statistic data of DNS queries in Ireland on their website.

It is very hard to collect the records about all DNS queries, because there are numerous recursive DNS servers and they are managed by many organizations [13], hence,

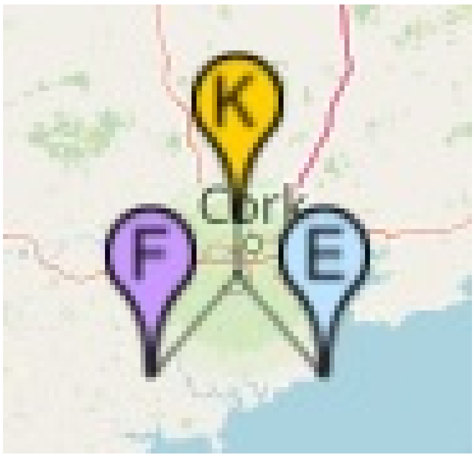


Figure 3.3: *The root servers in Cork [1]*

Zone	Operator	Number in Ireland
A	Verisign	0
B	USC-ISI	0
C	Cogent Communications	0
D	University of Maryland	1
E	NASA Ames Research Center	3
F	Internet Systems Consortium	2
G	Defense Information Systems Agency	0
H	U.S. Army Research Lab	0
I	Netnod	0
J	Verisign	1
K	RIPE NCC	1
L	ICANN	0
M	WIDE Project	0

Table 3.1: The list of root server zones [1]

the operators of root servers do not have their data.

However, it is not necessary to know the total number of DNS queries in Ireland, because the target in this research is to understand what the performance should a TTR server possess in Ireland. The number of DNS queries a root server may receive can help us to evaluate the required performance for a TTR server in Ireland.

In this paper, the researcher designs some methods to estimate the traffic a DNS server would have in Ireland by using the traffic in root servers.

Method 1 is using the data on Akamai.com to estimate the DNS traffic [2].

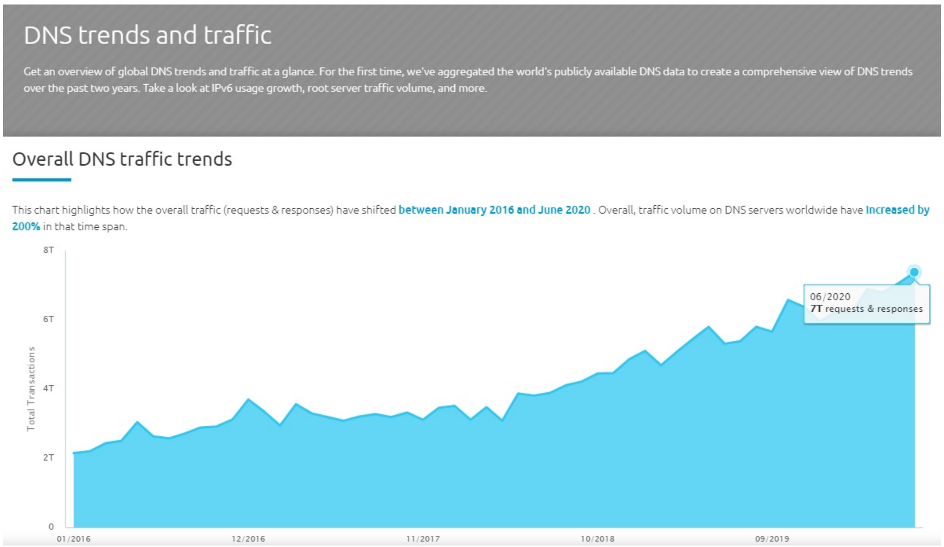
In website Akamai.com, it collects the DNS traffic from 9 root server zones(B, C, D, E, F, I, K, L, M), but the DNS traffic is worldwide, it does not provide the data in national scale or city scale on the website.

Even though there is no national scale data on Akamai.com, but the worldwide data can be used to estimate the Irish DNS traffic.

In a report from Central Statistics Office of Ireland, it showed that there were 89% of Irish households have the internet at home in 2018 [14]. From the growth of households with the internet, the percentage is probably 90% in 2020. There were about 4.57 billion internet users in the world in July 2020 [15]. The population in Ireland was around 4.944 million in August 2020 [16]. Hence, the Irish Internet users may be about 4.113 million, it was approximately 0.09% of internet users in the whole world.

According to the data from Akamai.com [2], the overall DNS traffic in the world was about 7 Trillion transactions (Requests and responses) in June 2020. Then, 0.09% of DNS traffic in the world could be Irish DNS traffic, which is around 6.3 billion DNS transactions for one month in Ireland. On average, it could be 210 DNS million transactions in a day in Ireland.

However, internet traffic is changeable in different hours, it is necessary to understand when are the rush hours. For example, the internet rush hours are usually between 7 pm and 11 pm in UK [17]. In Sao Paulo, the internet rush hours are between 8 pm and 11 pm [18]. In USA, it is 8 pm to 10 pm [19]. In Berlin, the rush hours are



DNS trends and traffic

Get an overview of global DNS trends and traffic at a glance. For the first time, we've aggregated the world's publicly available DNS data to create a comprehensive view of DNS trends over the past two years. Take a look at IPv6 usage growth, root server traffic volume, and more.

Overall DNS traffic trends

This chart highlights how the overall traffic (requests & responses) have shifted **between January 2016 and June 2020** . Overall, traffic volume on DNS servers worldwide have **Increased by 200%** in that time span.

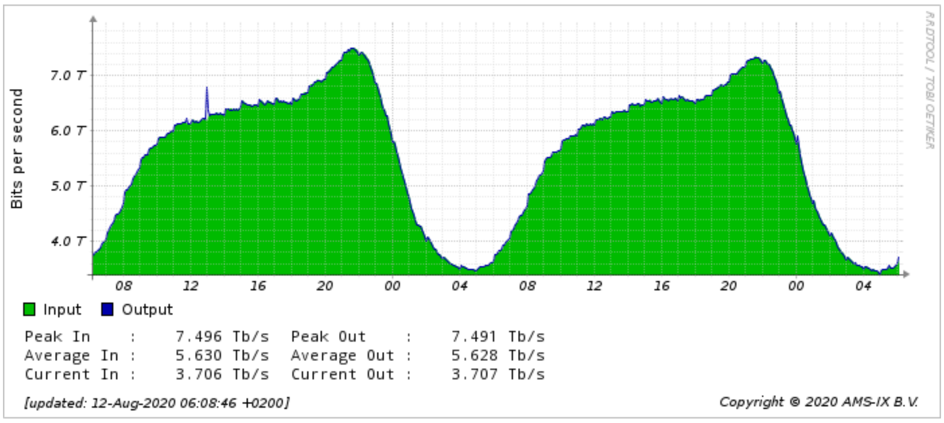
Figure 3.4: *The trend of DNS traffic in the world [2]*

Month	IPv4	IPv6	Total
06/2020	6T	1T	7T
01/2020	5T	969B	6T
07/2019	4T	919B	5T
01/2019	4T	848B	5T
07/2018	3T	564B	4T
01/2018	3T	426B	4T
07/2017	3T	371B	3T
01/2017	3T	363B	3T
07/2016	2T	248B	3T
01/2016	2T	171B	2T

Table 3.2: Overall DNS traffic trends(Unit:Transactions) [2]

8 pm to 11 pm [20]. In Amsterdam, it is from 8 pm to 11 pm as well [3].

All the reports in different countries or cities revealed that internet rush hours are from 8 pm to 11 pm, the distributions are pretty similar. Therefore, Irish internet rush hours could be assumed as from 8 pm to 11 pm as well.

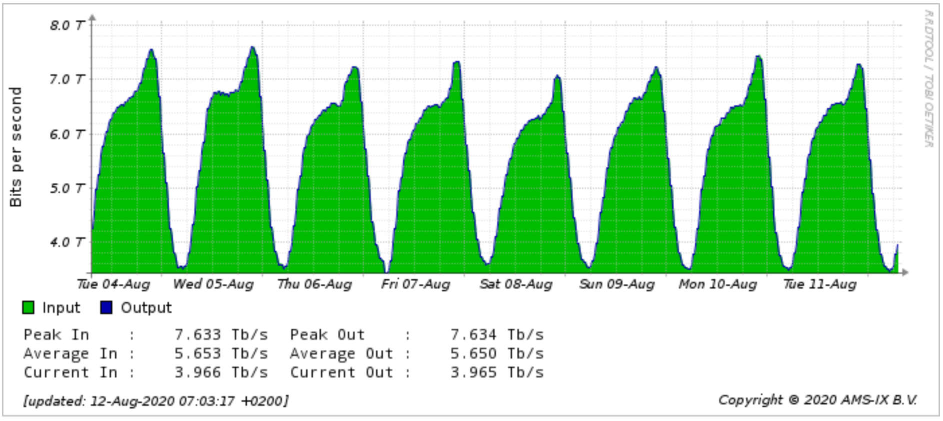


```
Peak In     :    7.496 Tb/s  Peak Out     :    7.491 Tb/s
Average In  :    5.630 Tb/s  Average Out  :    5.628 Tb/s
Current In  :    3.706 Tb/s  Current Out  :    3.707 Tb/s
```

[updated: 12-Aug-2020 06:08:46 +0200]

Copyright © 2020 AMS-IX B.V.

Figure 3.5: *The internet traffic in a day (Amsterdam) [3]*



```
Peak In     :    7.633 Tb/s  Peak Out     :    7.634 Tb/s
Average In  :    5.653 Tb/s  Average Out  :    5.650 Tb/s
Current In  :    3.966 Tb/s  Current Out  :    3.965 Tb/s
```

[updated: 12-Aug-2020 07:03:17 +0200]

Copyright © 2020 AMS-IX B.V.

Figure 3.6: *The internet traffic in a week (Amsterdam) [3]*

As for the comparison in different days in a week, from Monday to Sunday, the change is not obvious. About the days in a month, from the begin to the end of a month, there is no huge difference as well.

Taking the data in Amsterdam to estimate the percentage of usage in each hour, the result is shown in TABLE 3.3.

After that, using the percentage to multiply the estimated number of daily DNS transactions in Ireland, which is 210 million, then the result is sown in TABLE 3.4.

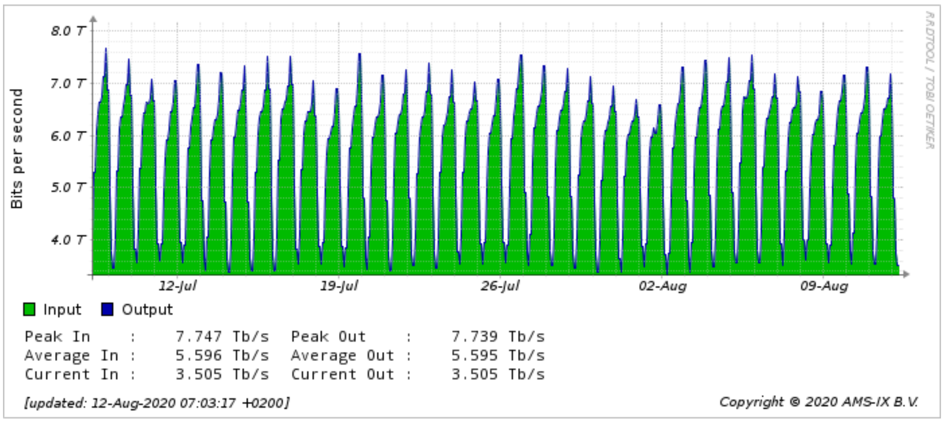


Figure 3.7: *The internet traffic in a month (Amsterdam) [3]*

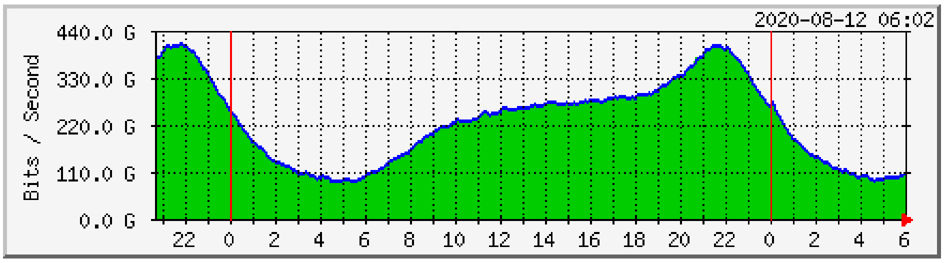


Figure 3.8: *The internet traffic in a day (Berlin) [3]*

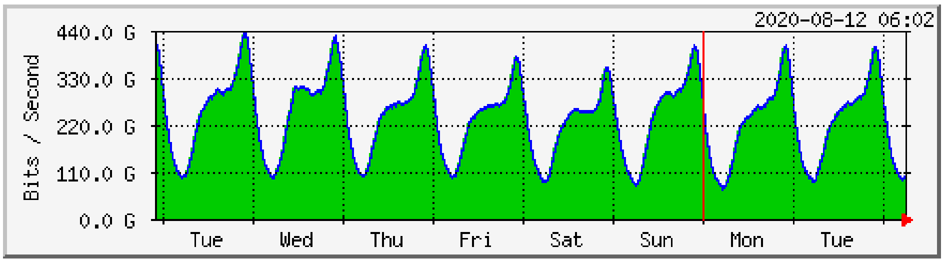


Figure 3.9: *The internet traffic in a week (Berlin) [3]*

The 2 busiest hours are 9 PM and 10 PM, the number of DNS transactions could be 11.2 million in an hour.

However, the data from Akamai.com does not include A, G, H and J root server zones. Thus, the number of transactions in rush hours should be higher than 11.2 million.

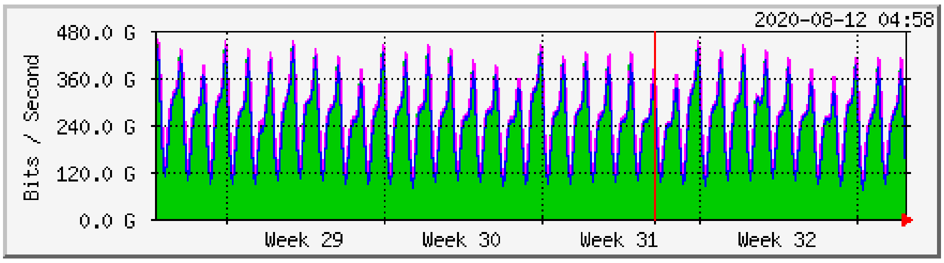


Figure 3.10: *The internet traffic in a month (Berlin) [3]*

Hour(24)	Trillion bit/s	Percentage
0	5.8	4.3%
1	4.8	3.56%
2	4	2.96%
3	3.7	2.74%
4	3.6	2.67%
5	3.5	2.59%
6	3.6	2.67%
7	4	2.96%
8	4.8	3.56%
9	5.4	4%
10	5.8	4.3%
11	6	4.44%
12	6.2	4.59%
13	6.4	4.74%
14	6.4	4.74%
15	6.6	4.89%
16	6.6	4.89%
17	6.6	4.89%
18	6.5	4.81%
19	6.7	4.96%
20	6.9	5.11%
21	7.2	5.33%
22	7.2	5.33%
23	6.7	4.96%
Total	135	100%

Table 3.3: Internet traffic and its percentage in each hour in a day in Amsterdam [3]

Hour(24)	Percentage	Million transactions
0	4.3%	9.02
1	3.56%	7.47
2	2.96%	6.22
3	2.74%	5.76
4	2.67%	5.6
5	2.59%	5.44
6	2.67%	5.6
7	2.96%	6.22
8	3.56%	7.47
9	4%	8.4
10	4.3%	9.02
11	4.44%	9.33
12	4.59%	9.64
13	4.74%	9.96
14	4.74%	9.96
15	4.89%	10.27
16	4.89%	10.27
17	4.89%	10.27
18	4.81%	10.11
19	4.96%	10.42
20	5.11%	10.73
21	5.33%	11.2
22	5.33%	11.2
23	4.96%	10.42
Total	100%	210

Table 3.4: Using the daily distribution of Internet traffic of Amsterdam to estimate the DNS traffic in Ireland [3]

The numbers of transactions in every root server zone are very different, therefore it is hard to estimate the numbers in A, G, H and J root server zones. If assume that the average number of A, G, H and J is close to the average number of B, C, D, E, F, I, K, L, M, then the estimated number of transactions in all root servers in rush hours could be 11.2/9X13=16.18 million.

If convert it into a second, the number of DNS transactions could be 4,494 per second during the rush hour (16.18(million per hour)/60(minutes)/60(seconds)).

Method 2 is using the data from ICANN to estimate DNS traffic.

ICANN (Internet Corporation for Assigned Names and Numbers) is the one of 12 organizations which are responsible for managing DNS root servers, the servers it manages are L-root servers. Unlike other 11 organizations, ICANN provides a website to display real-time DNS traffic, that is Stats.dns.icann.org [5].

The problem is ICANN does not have root servers in Ireland. Moreover, those data is only from ICANN, it does not include the data from other root server zones.

Thus, here chose a city which has a similar population to Ireland to estimate the DNS traffic. Melbourne should be a ideal sample. The population in Melbourne is about 5 million in 2019 [21], which is close to the population in Ireland (4.9 million). Moreover, Melbourne is isolated, there is no big city near Melbourne,therefore the network connection may be similar to a country.

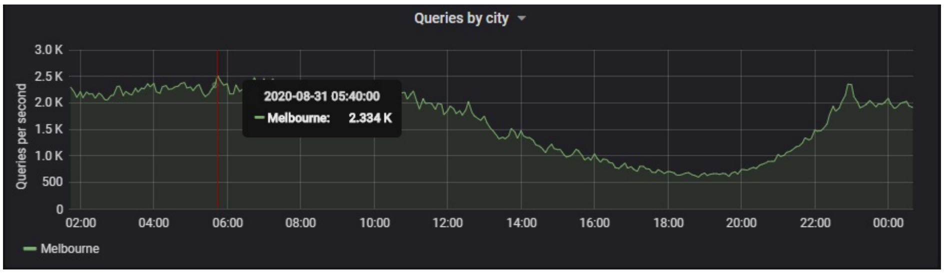


Figure 3.11: *The number of queries per second in a root server in Melbourne [5]*

From the data in Fig. 3.11, the highest value in a day is 2,334 per second, which was occurred at 05:40 UTC(19:40 in Melbourne).

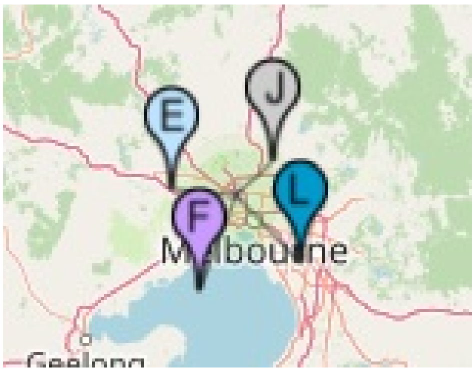


Figure 3.12: *The root servers in Melbourne [1]*

However, the data is only from a root server which is managed by ICANN, there are four root servers in Melbourne, the DNS traffic in other 3 root servers are not provided. Assume the average traffic in other 3 root servers is close to the root server managed by ICANN, the whole DNS traffic in Melbourne could be 9,336 per second(2,334X4). Next, adjust the traffic to accord the population of Ireland, the DNS traffic could be 9,149 per second during the rush hour(9,336/5X4.9).

The comparison between method 1 and method 2 is shown in TABLE 3.5.

	Method 1	Method 2
Source	Akamai.com	ICANN
Queries per second in rush hours	4,494	9,149
Drawback 1	No Irish data	No Irish data
Drawback 2	Only monthly data	The data is only from L-root

Table 3.5: The comparison between 2 methods for the estimation of the DNS traffic in Ireland

3.1 Section 1.1

...

Chapter 4

Required software

4.1 The overview of required software

Building a DNS server for TRR needs some software, including the software for implementing DNS server, operation system, tools and server [22].

The DNS server need tools to recieve DoH queries and test. DoH-proxy is designed for this purpose, the developer is Facebook. It can be installed on Linux but it requires Python 3.5 [23].

After that, NGINX can provide the web service. NGINX is a HTTP server with high performance, it can also provide different kinds of services. The operator can set the method for listening queries in a port and the request from users [24].

About Operating System, Linux is recommended, because the much resource for building DNS servers is based on Linux [25].

The required software is shown in TABLE 4.1.

Category	Software	Note
DNS	BIND 9	
DNS	Unbound	Free and open-source software
DNS	PowerDNS	
Tool	DoH-proxy	
Server	NGINX	Free and open-source software

Table 4.1: The required software for building a DNS server for TRR

4.2 Comparison of DNS software

There are many choices to implement a DNS server, such as BIND, Unbound, DNSMASQ, PowerDNS, Microsoft DNS and Cisco Network Registrar [26] [27]. In this research, Unbound, BIND and PowerDNS are recommended, because there are many discussion about those three software on Internet, moreover, they support DNS over HTTPS (DoH), then users may use TRR to browse websites in Firefox [28] [29].

Unbound is the free open-source software which focuses on building a recursive DNS server, it does not support the authoritative DNS server. The developer is NLnet Labs, the developer also designed another DNS software, which is NSD(Name Server Daemon), in contrast, NSD is only for building authoritative DNS servers [30]. Unbound supports some security functions, such as Domain Name System Security Extensions(DNSSEC) and DNS over TLS(DoT). Moreover, the operating systems for running Unbound can be Linux, FreeBSD and Windows [31].

About BIND, its alias is Named. Unlike Unbound, it supports both recursive and authoritative DNS servers. It is developed by Internet Systems Consortium(ISC). ISC is also the organization which is responsible for managing F root server zone. The stable version is BIND 9. It can run on Windows, Mac-OS and Linux [32].

PowerDNS, it supports both authoritative DNS server and recursive DNS server, moreover, it provides a Graphic UI for management and uses relational databases to store data. The developer is PowerDNS Community and operating systems are Linux and FreeBSD [33].

Compare with Unbound, BIND and PowerDNS, those three software are all good choices [34].

For the consideration about the performance, there are some difference among BIND, Unbound and PowerDNS.

According to a report which was written by Hamza Boulakhrif in University of Amsterdam, The times for processing queries in BIND, Unbound and PowerDNS were similar. The biggest difference was that when the time of processing exceeded 16 seconds, then PowerDNS did not response. If the time exceeded 17 seconds, BIND did not response, only Unbound can wait until the finish of processing then sent results to users [6].

The processing time in those 3 DNS software in this report is shown in Fig. 4.1.

In Fig. 4.1, according to the assumption of Hamza Boulakhrif, if processing time is under 1 milliseconds, then it is processed by the cache, because the caches in DNS servers contain the matched IP addresses that users are looking for, thus DNS servers can response users in a very short time and do not need to ask authoritative DNS servers.

In the other experiment, BIND, Unbound and PowerDNS ran with DNSSEC, there

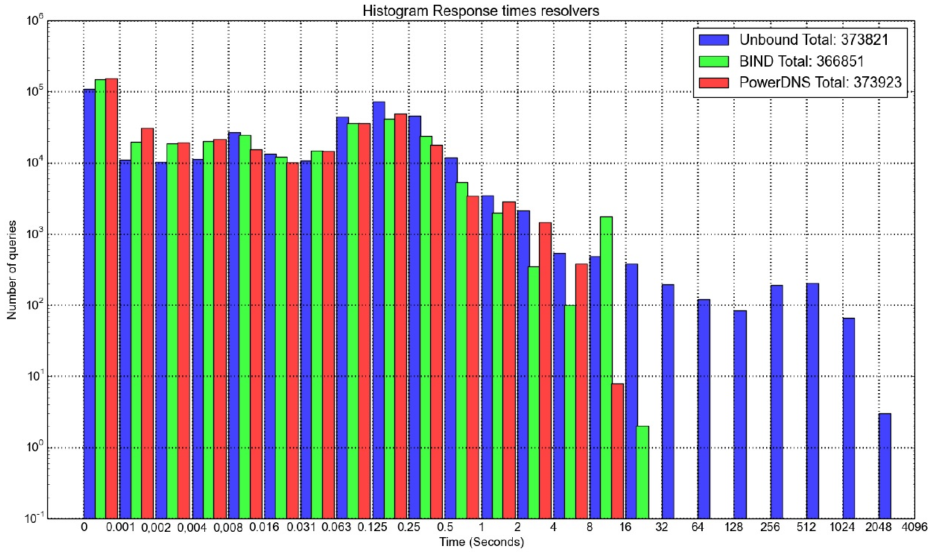


Figure 4.1: *The processing time in BIND, Unbound and PowerDNS [6]*

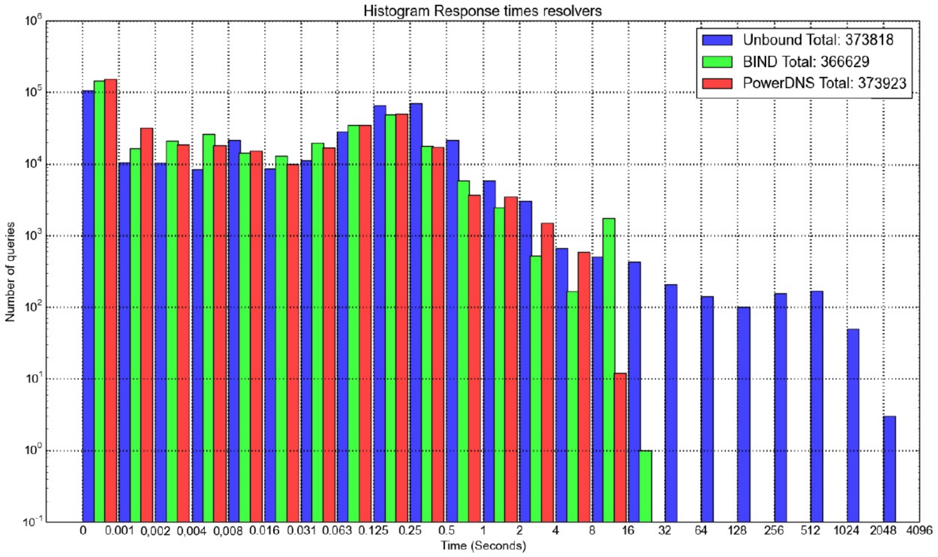


Figure 4.2: *The processing time in BIND, Unbound and PowerDNS with DNSSEC [6]*

was no obvious change if compare it with these DNS servers without DNSSEC. The result of using DNSSEC is shown in Fig. 4.2.

Fig. 4.4, Fig. 4.5 and Fig. 4.3 show the details of the time of processing queries

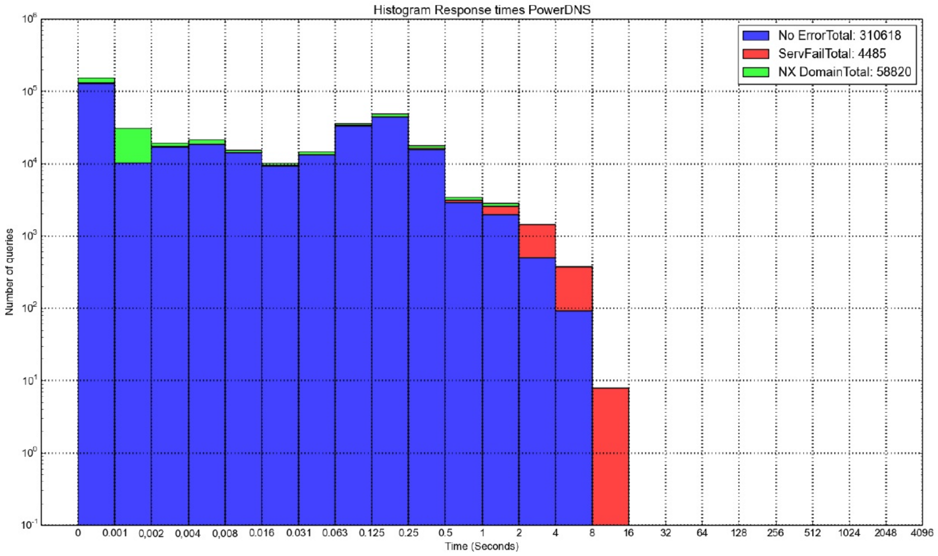


Figure 4.3: *The processing time in PowerDNS [6]*

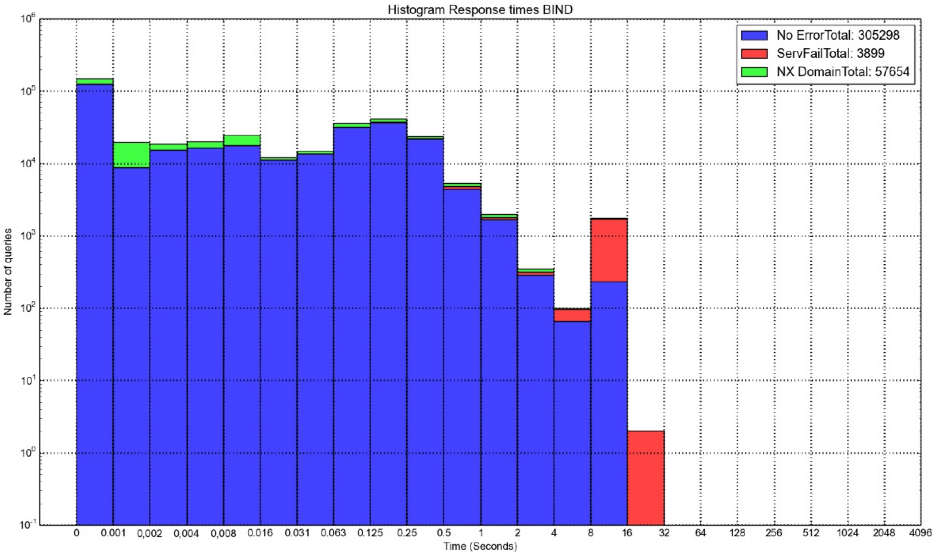


Figure 4.4: *The processing time in BIND [6]*

in BIND, Unbound and PowerDNS. The working types in BIND and PowerDNS are similar, both of them have the time limit, thus in case the processing time reaches the time limit, then the query will be failed. In contrast, Unbound has a different working type, it allows the system to have a long time to wait for the answer after the

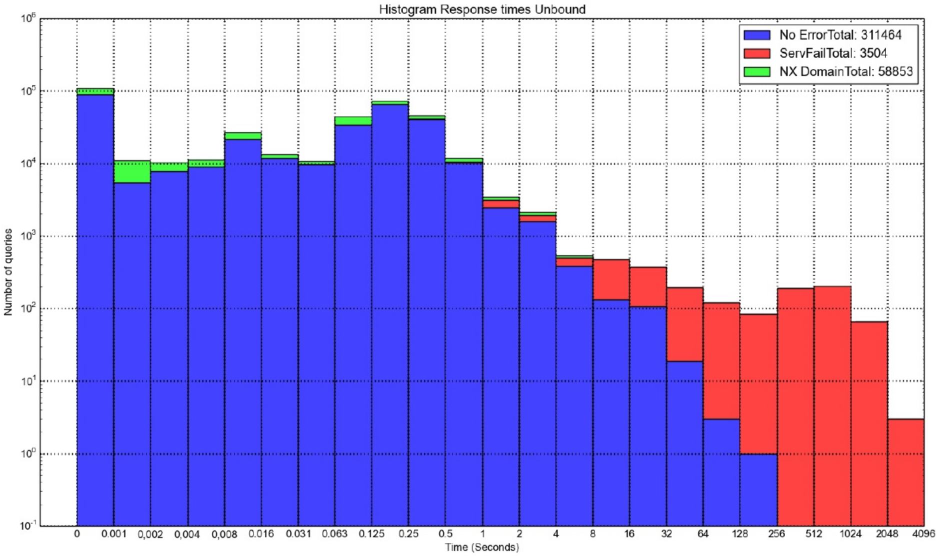


Figure 4.5: *The processing time in Unbound [6]*

process. Hamza Boulakhrif called those different working types as ”Failed response over a late response” and ”An answer is better than no answer”. PowerDNS adopts ”Failed response over a late response” and Unbound adopts ”An answer is better than no answer”, as for BIND, it is between PowerDNS and Unbound [6].

In conclusion, in choosing DNS resolver software, because BIND, Unbound, PowerDNS have similar performances, therefore the point of the decision is allowing a long time to wait for the answer or not. If yes, the operator should choose Unbound. Otherwise, he should choose BIND or PowerDNS.

However, the report was written in 2015, which was 5 years ago, the situation may be different now.

4.3 Comparison of operating system

In choosing a operation system for testing, there are many operation systems could be used to install DNS servers, such as Windows server, BSD, Linux Red Hat, Linux Ubuntu, Linux CentOS. Many developers prefer using Unix-like rather than Windows server base on the concern about stability and cost, therefore the researcher excluded Windows server.

On the other hand, even though FreeBSB is a good choice for building servers, but the information of BSD is less than Linux, which means Linux is more popular, thus the researcher decided to use Linux.

However, there are many members in the Linux family, including Fedora,Red Hat Linux, CentOS, Ubuntu, Debian [35]. CentOS is chosen here, because it is free, and the structure is the offshoot of Red Hat enterprise, hence it is very stable.

4.4 Installing a DOH server for TRR

After the discussion about the performance, in order to understand the situation of the setting and usability among BIND, Unbound and PowerDNS, the researcher tried to install those 3 DNS software on a server and test them.

Due to the effect of COVID-19, students were not allowed to go inside the laboratory, hence this study has to be finished at home, therefore the equipment was limited, only 4 personal devices were available to the researcher, which were a personal desktop computer, 2 android phones and a IPad. The operating system on the personal desktop computer is Windows 10. Thus, there was no spare computer to install Linux, the researcher had to use a virtual machine to install Linux on the personal computer.

The software for running virtual machine was VMware Workstation Player.

After installing the operation system, then installed BIND, Unbound and PowerDNS, and set the configuration files of those DNS servers, to make sure those DNS servers were in the same network zone with other testing devices.

Next, used Internet Information Services(IIS) to create a simple website on the personal computer, and gave fixed local IP addresses to all devices and the virtual machine, then both the DNS server and website had the IP addresses. In the DNS server(BIND, Unbound and PowerDNS), set a domain name to the simple website to match its IP address. The simple website was the testing website.

Finally, used the testing devices(Android phone and IPad) to type the domain name of the testing website on browsers(Google Chrome and Safari). If the testing website could be displayed on testing devices, then the DNS server functioned well.

Above steps were the testing method for the study. The testing environment is shown in TABLE 4.2.

Platform	VMware Workstation 15.5.6 Player
Operating system	CentOS 8.2.2004
Internet connection	Bridge mode
Testing devices	Desktop, IPad, Android phone

Table 4.2: The testing environment

Next, the following discussion is about configuration. The configuration of BIND is using C language to be the format of the configuration file. Therefore, in case the maintenance personnel does not have programming background, then it needs time to understand the syntax of C language.

About Unbound, the format of configuration file is very simple, it does not belong to any kind of computer languages. The setting is just listed line by line.

PowerDNS adopts relational database, thus the configuration of PowerDNS has 2 parts, the first part is the normal configuration file, it decides the setting for the database. The second part is in the database, the contain is including domains and records.

The installation of PowerDNS is more complex than Unbound and BIND, because it uses the rational database. However, it is a double-edged sword, it is not friendly for normal users during the installation, but after installation, PowerDNS provides the website to display the information of DNS server, and the website is also the interface for the setting, hence the maintenance is easier than BIND and Unbound.

The comparison among BIND, Unbound, PowerDNS is shown in Table 4.3.

	BIND	Unbound	PowerDNS
Version			
Query time limit	Short	Long	Short
Performance	Similar	Similar	Similar
Configuration	C language	Line by line	RDBMS
Log style	Log file	Log file	MySQL
Installation difficulty	Easy	Easy	Difficult
Maintenance difficulty	Normal	Normal	Easy

Table 4.3: The comparison among BIND, Unbound, PowerDNS

4.5 The simulation of the internet traffic in national scale

In previous description, a DNS server is possible to suffer 4,494 transactions per second, therefore it is necessary to simulate this situation to the DNS server which is built by the researcher.

The researcher used Python to make a simple application, the application can send a huge number of queries to the DNS server, and the number can be changed by the researcher.

Language	Python 3.7
Library	DNS.resolver
DNS software	BIND
CPU in the server	Intel Core i7-7700(3.60GHz, 4 cores)
Memory in the server	8G
Operating system	CentOS 8.2 in virtual machine
First testing	100 queries for 1 domain name
Second testing	5000 queries for 1 domain name
Third testing	10000 queries for 1 domain name
Forth testing	100 queries for different domain names
Fifth testing	5000 queries for different domain names
Sixth testing	10000 queries for different domain names

Table 4.4: The description of the application for testing massive queries

Chapter 5

Other concerns

5.1 The concern of DDOS attacks

DDOS is the important issue for building DNS server.

There are 2 sorts of DNS queries, recursive and iterative. At the beginning, users send queries to recursive servers, when recursive DNS servers receive requests, if they do not have the matched IP addresses, then recursive DNS servers can help users to ask authoritative DNS servers for getting IP addresses, then return results to users, that is the recursive query.

As for the iterative query, when authoritative DNS servers receive the queries from recursive DNS servers, if they do not have the matched IP addresses, they will give recursive servers the IP addresses of other authoritative DNS servers for querying, then recursive servers will ask other authoritative DNS servers, this type of querying is the iterative query [36].

However, the recursive queries may cause DDOS attacks. The content of packet could be faked, the IP address of a sender can be changed to be the IP address of the victim. In case thousands of computers send recursive queries to DNS servers, and all IPs of sources are changed to be the IP of a victim, then those DNS servers will send thousands of responses to that victim. After that, the traffic in the victim would be too high then cause some problems [7]. This type of DDOS attack is called DNS amplification attack [37].

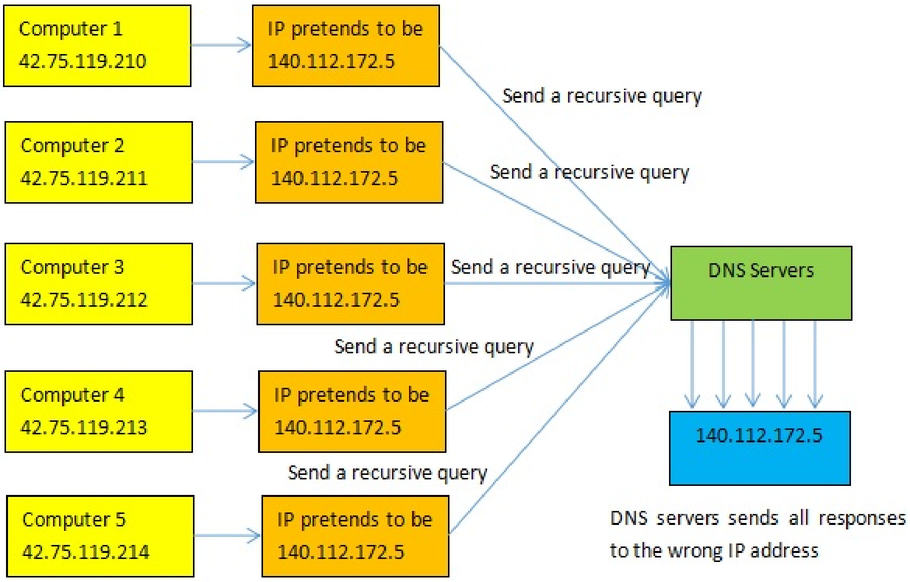


Figure 5.1: *The DDOS attack in recursive DNS queries [7]*

Thus, restricting DNS queries may be the ideal method to prevent DNS amplification attacks, the implementation is to disable the recursion for everyone, only local queries are allowed to be processed [38].

5.2 The required performance

A DNS transaction contains many packets.

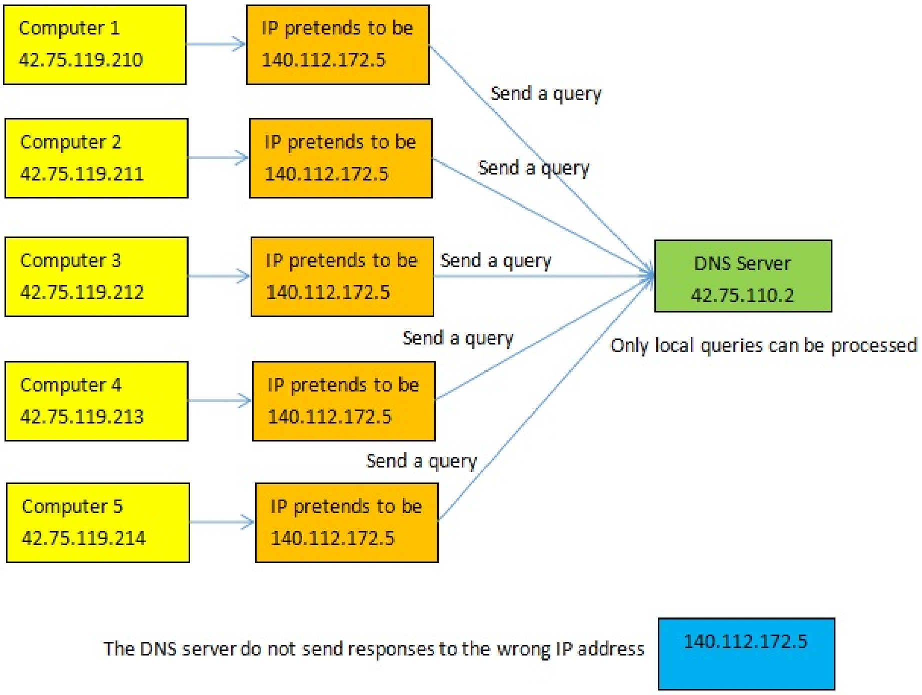


Figure 5.2: *Restricting DNS queries to prevent DNS amplification attacks [7]*

5.3 The concern of disasters

COVID-19

Chapter 6

Overall design

...

Bibliography

[1] root servers.org, “root-servers.org.” [Online]. Available: https://root-servers.org/.

[2] Akamai.com, “Dns trends and traffic.” [Online]. Available: https://www.akamai.com/de/de/why-akamai/dns-trends-and-traffic.jsp.

[3] AMS-IX, “Total traffic statistics(amsterdam).” [Online]. Available: https://stats.ams-ix.net/index.html.

[4] Cloudflare, “What is a dns root server?.” [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/dns-root-server/.

[5] stats.dns.icann.org, “stats.dns.icann.org.” [Online]. Available: https://stats.dns.icann.org/.

[6] W. T. Hamza Boulakhrif, Yuri Schaeffer, “Analysis of dns resolver performance measurements,” tech. rep., University of Amsterdam, July 2015.

[7] F. Internet, “What is recursive dns and why is it not recommended for most server owners?.” [Online]. Available: https://www.youtube.com/watch?v=W3wXkHAv3qo.

[8] Wikipedia, “Ipv4.” [Online]. Available: https://en.wikipedia.org/wiki/IPv4.

[9] Wikipedia, “Ipv6.” [Online]. Available: https://en.wikipedia.org/wiki/IPv6.

[10] Wikipedia, “Domain name.” [Online]. Available: https://en.wikipedia.org/wiki/Domain_name.

[11] J. Peters, "What is dns, how it works + vulnerabilities." [Online]. Available: `https://www.varonis.com/blog/what-is-dns/`.

[12] Wikipedia, "Root name server." [Online]. Available: https://en.wikipedia.org/wiki/Root name server.

[13] D. M. Easy, "What is the difference between authoritative and recursive dns nameservers?." [Online]. Available: `https://umbrella.cisco.com/blog/what-is-the-difference-between-authoritative-and-recursive-dns-nameservers`.

[14] central statistics office (Ireland), "Information society statistics - households." [Online]. Available: https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2018/.

[15] J. Clement, "Global digital population as of july 2020." [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/.

[16] Worldometer, "Ireland population(live)." [Online]. Available: https://www.worldometers.info/world-population/ireland-population/.

[17] N. Cumins, "Avoiding the internet rush hour." [Online]. Available: https://broadbanddeals.co.uk/avoiding-the-internet-rush-hour/.

[18] ix.br, "Selecione a localidade para ver as estatísticas de tráfego." [Online]. Available: https://ix.br/trafego/agregado/sp.

[19] federal communications commission, "Measuring broadband america-july 2012." [Online]. Available: https://www.fcc.gov/reports-research/reports/measuring-broadband-america/measuring-broadband-america-july-2012.

[20] DE-CIX, "Traffic statistics(berlin)." [Online]. Available: https://www.bcix.de/bcix/traffic/.

[21] Wikipedia, "Melbourne." [Online]. Available: https://en.wikipedia.org/wiki/Melbourne.

[22] Loull, "Dns resources." [Online]. Available: https://www.cnblogs.com/549294286/p/5200255.

[23] Facebookexperimental, "Dns over https proxy." [Online]. Available: https://github.com/facebookexperimental/doh-proxy.

[24] NGINX, "Welcome to niginx wiki!." [Online]. Available: https://www.nginx.com/resources/wiki/.

[25] M. Anicas, "How to configure bind as a private network dns server on ubuntu 14.04." [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-14-04.

[26] Wikipedia, "Comparison of dns server software." [Online]. Available: https://en.wikipedia.org/wiki/Comparison of DNS server software.

[27] K. John, "Bind vs dnsmasq vs powerdns vs unbound." [Online]. Available: https://computingforgeeks.com/bind-vs-dnsmasq-vs-powerdns-vs-unbound/.

[28] ISHM, "Building dns over https server on centos 7." [Online]. Available: https://ishm.idv.tw/?p=481.

[29] Archlinux, "Dns over https servers." [Online]. Available: https://wiki.archlinux.org/index.php/DNS_over_HTTPS_servers.

[30] Wikipedia, "Nsd." [Online]. Available: https://en.wikipedia.org/wiki/NSD.

[31] Wikipedia, "Unbound (dns server)." [Online]. Available: https://en.wikipedia.org/wiki/Unbound(DNS_server).

[32] Wikipedia, "Bind." [Online]. Available: https://en.wikipedia.org/wiki/BIND.

[33] Wikipedia, "Powerdns." [Online]. Available: https://en.wikipedia.org/wiki/PowerDNS.

[34] TINYDNS, "Compare the different dns servers: Which one is right for you?." [Online]. Available: https://tinydns.org/compare-different-dns-servers/.

[35] Wikipedia, "List of linux distributions." [Online]. Available: https://en.wikipedia.org/wiki/List_of_Linux_distributions.

[36] Cloudflare, “What is recursive dns?.” [Online]. Available: `https://www.cloudflare.com/learning/dns/what-is-recursive-dns/`.

[37] Imperva, “Dns amplification.” [Online]. Available: `https://www.imperva.com/learn/ddos/dns-amplification/`.

[38] F. Internet, “What is recursive dns and why is it not recommended?.” [Online]. Available: `https://help.fasthosts.co.uk/app/answers/detail/a_id/1276`.

Appendix

...