

Comunicações por Computador

Trabalho Prático 3

Hugo Cardoso (A85006)

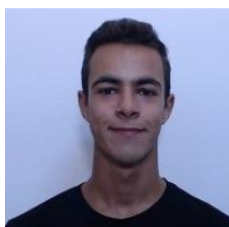
João Costa (A84775)

Válter Carvalho (A84464)

15 de Abril de 2020



Escola de Engenharia



Grupo 02 - PL4

Mestrado Integrado em Engenharia Informática

Universidade do Minho

Conteúdo

1	Introdução	2
2	Parte 1	3
3	Parte 2	18
3.1	Servidor Primário	18
3.2	Servidor Secundário	22
3.3	Testes e Demonstrações	24
4	Conclusão	29

1 Introdução

O DNS é um serviço que, numa forma simplista, permite gerir os nomes associado a um endereço IP, de forma hierárquica, isto é, servidores relativos a: raiz, domínios de topo e os autoritários.

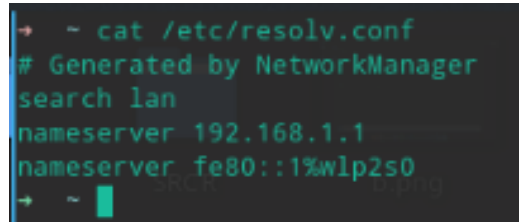
Os servidor de raiz (.) são o topo da hierarquia e têm a função de responder pedidos dos seus registos assim como os seus servidores de topo.

Os servidores de topo (**.pt**, **.org**, **.com**, ...) conhecem os endereços dos servidores autoritativos pertencentes a si mesmo e respondem a questões associadas a pedidos dos seus registos assim como indicar o servidor autoritativo correto. Os servidores autoritativos (**uminho**, **youtube**, ...) têm como função, como o nome indica, a gestão dos subdomínios (**di.uminho**, **music.youtube**, ...) assim como o próprio domínio associados.

A proposta da equipa docente foi testar usando um ambiente UNIX a forma como funciona o DNS numa forma mais interativa, que foi o objetivo principal deste trabalho prático, que passou, numa primeira fase, por uma parte mais teórica seguida duma parte mais prática, que realizamos o nosso próprio servidor de DNS numa topologia CORE.

2 Parte 1

- (a) Qual o conteúdo do ficheiro `/etc/resolv.conf` e para que serve essa informação?

A terminal window with a dark background and light green text. The command `cat /etc/resolv.conf` has been executed. The output shows the following lines: `# Generated by NetworkManager`, `search lan`, `nameserver 192.168.1.1`, and `nameserver fe80::1%wlp2s0`. The prompt `→ ~` is visible at the bottom left.

```
→ ~ cat /etc/resolv.conf
# Generated by NetworkManager
search lan
nameserver 192.168.1.1
nameserver fe80::1%wlp2s0
→ ~
```

Como podemos ver temos 2 parâmetros:

- **search:** quando numa query de resolução de nomes não for indicado um domínio (por exemplo, colocando algo incompleto como *youtube/subscriptions*, o nome indicado será auto-completado com o campo *lan*, isto é, *youtube.lan/subscriptions*);
- **nameserver:** endereço IPv4 e IPv6 do servidor de DNS local a que serão enviadas todas as queries.

- (b) Os servidores **www.sapo.pt.** e **www.yahoo.com.** têm endereços IPv6? Se sim, quais?

Como vemos nas seguintes imagens os endereços IPv6 associados a **www.sapo.pt** e **www.yahoo.com** são:

- **www.sapo.pt:** 2001:8a0:2102:c:213:13:146:142

```
+ ~ dig www.sapo.pt AAAA

; <<>> DiG 9.16.1 <<>> www.sapo.pt AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3836
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sapo.pt.                IN      AAAA

;; ANSWER SECTION:
www.sapo.pt.                261     IN      AAAA    2001:8a0:2102:c:213:13:146:142

;; AUTHORITY SECTION:
sapo.pt.                    2080    IN      NS      ns.sapo.pt.
sapo.pt.                    2080    IN      NS      ns2.sapo.pt.
sapo.pt.                    2080    IN      NS      dns01.sapo.pt.
sapo.pt.                    2080    IN      NS      dns02.sapo.pt.

;; ADDITIONAL SECTION:
ns.sapo.pt.                 10009   IN      A       212.55.154.202
ns2.sapo.pt.                9656    IN      A       212.55.154.194
dns01.sapo.pt.              597     IN      A       213.13.28.116
dns02.sapo.pt.              6409    IN      A       213.13.30.116
dns01.sapo.pt.              2080    IN      AAAA    2001:8a0:2106:4:213:13:28:116
dns02.sapo.pt.              897     IN      AAAA    2001:8a0:2206:4:213:13:30:116

;; Query time: 10 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: qua abr 15 08:52:42 WEST 2020
;; MSG SIZE rcvd: 263

+ ~ █
```

- **www.yahoo.com:**
 - 2a00:1288:110:1c::4;
 - 2a00:1288:110:1c::3.

```

→ ~ dig www.yahoo.com AAAA

; <<>> DiG 9.16.1 <<>> www.yahoo.com AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53878
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yahoo.com.                IN      AAAA

;; ANSWER SECTION:
www.yahoo.com.                1398    IN      CNAME   atsv2-fp-shed.wg1.b.yahoo.com.
atsv2-fp-shed.wg1.b.yahoo.com. 7 IN     AAAA    2a00:1288:110:1c::4
atsv2-fp-shed.wg1.b.yahoo.com. 7 IN     AAAA    2a00:1288:110:1c::3

;; AUTHORITY SECTION:
wg1.b.yahoo.com.              6556    IN      NS       yf4.a1.b.yahoo.net.
wg1.b.yahoo.com.              6556    IN      NS       yf3.a1.b.yahoo.net.
wg1.b.yahoo.com.              6556    IN      NS       yf2.yahoo.com.
wg1.b.yahoo.com.              6556    IN      NS       yf1.yahoo.com.

;; ADDITIONAL SECTION:
yf1.yahoo.com.                3991    IN      A        68.142.254.15
yf4.a1.b.yahoo.net.           4021    IN      A        68.180.130.15
yf2.yahoo.com.                 3991    IN      A        68.180.130.15
yf3.a1.b.yahoo.net.           4021    IN      A        68.180.130.15

;; Query time: 13 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: qua abr 15 08:53:07 WEST 2020
;; MSG SIZE rcvd: 282

→ ~ █

```

(c) Quais os servidores de nomes definidos para os domínios: “uminho.pt.”, “pt.” e “.”?

Utilizando os comandos presentes nas imagens, obtivemos os seguintes nomes dos servidores definidos para os domínios:

- uminho.pt.:
 - ns02.fccn.pt;
 - dns3.uminho.pt;
 - dns.uminho.pt;
 - dns2.uminho.pt.

```

➔ ~ nslookup -type=ns uminho.pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
uminho.pt    nameserver = ns02.fccn.pt.
uminho.pt    nameserver = dns3.uminho.pt.
uminho.pt    nameserver = dns.uminho.pt.
uminho.pt    nameserver = dns2.uminho.pt.

Authoritative answers can be found from:
dns2.uminho.pt internet address = 193.137.16.145
dns.uminho.pt  internet address = 193.137.16.75
dns3.uminho.pt internet address = 193.137.16.65
ns02.fccn.pt   internet address = 193.136.2.228
dns2.uminho.pt has AAAA address 2001:690:2280:801::145
dns.uminho.pt  has AAAA address 2001:690:2280:1::75
dns3.uminho.pt has AAAA address 2001:690:2280:1::65
ns02.fccn.pt   has AAAA address 2001:690:a80:4001::200
➔ ~ █

```

- pt.:
 - a.dns.pt;
 - g.dns.pt;
 - f.dns.pt;
 - e.dns.pt;
 - ns2.nic.fr;
 - h.dns.pt;
 - c.dns.pt;
 - d.dns.pt;
 - b.dns.pt;
 - ns.dns.br.

```

→ ~ nslookup -type=ns pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
pt          nameserver = a.dns.pt.
pt          nameserver = g.dns.pt.
pt          nameserver = f.dns.pt.
pt          nameserver = e.dns.pt.
pt          nameserver = ns2.nic.fr.
pt          nameserver = h.dns.pt.
pt          nameserver = c.dns.pt.
pt          nameserver = d.dns.pt.
pt          nameserver = b.dns.pt.
pt          nameserver = ns.dns.br.

Authoritative answers can be found from:
g.dns.pt    internet address = 193.136.2.226
ns.dns.br   internet address = 200.160.0.5
d.dns.pt    internet address = 185.39.210.1
ns2.nic.fr  internet address = 192.93.0.4
b.dns.pt    internet address = 194.0.25.23
c.dns.pt    internet address = 204.61.216.105
a.dns.pt    internet address = 185.39.208.1
f.dns.pt    internet address = 162.88.45.1
h.dns.pt    internet address = 194.146.106.138
e.dns.pt    internet address = 193.136.192.64
g.dns.pt    has AAAA address 2001:690:a80:4001::100
ns.dns.br   has AAAA address 2001:12ff:0:a20::5
d.dns.pt    has AAAA address 2a04:6d82::1
ns2.nic.fr  has AAAA address 2001:660:3005:1::1:2
b.dns.pt    has AAAA address 2001:678:20::23
→ ~ █

```

- .:
- j.root-servers.net;
- f.root-servers.net;
- l.root-servers.net;
- m.root-servers.net;
- k.root-servers.net;
- a.root-servers.net;
- b.root-servers.net;

- g.root-servers.net;
- d.root-servers.net;
- i.root-servers.net;
- c.root-servers.net;
- h.root-servers.net;
- e.root-servers.net.

```

➔ ~ nslookup -type=ns .
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
.           nameserver = j.root-servers.net.
.           nameserver = f.root-servers.net.
.           nameserver = l.root-servers.net.
.           nameserver = m.root-servers.net.
.           nameserver = k.root-servers.net.
.           nameserver = a.root-servers.net.
.           nameserver = b.root-servers.net.
.           nameserver = g.root-servers.net.
.           nameserver = d.root-servers.net.
.           nameserver = i.root-servers.net.
.           nameserver = c.root-servers.net.
.           nameserver = h.root-servers.net.
.           nameserver = e.root-servers.net.

Authoritative answers can be found from:
a.root-servers.net      internet address = 198.41.0.4
b.root-servers.net      internet address = 199.9.14.201
c.root-servers.net      internet address = 192.33.4.12
d.root-servers.net      internet address = 199.7.91.13
e.root-servers.net      internet address = 192.203.230.10
f.root-servers.net      internet address = 192.5.5.241
g.root-servers.net      internet address = 192.112.36.4
h.root-servers.net      internet address = 198.97.190.53
i.root-servers.net      internet address = 192.36.148.17
j.root-servers.net      internet address = 192.58.128.30
k.root-servers.net      internet address = 193.0.14.129
l.root-servers.net      internet address = 199.7.83.42
m.root-servers.net      internet address = 202.12.27.33
a.root-servers.net      has AAAA address 2001:503:ba3e::2:30
b.root-servers.net      has AAAA address 2001:500:200::b
➔ ~ █

```

(d) Existe o domínio nice.software.? Será que nice.software. é um host ou um domínio?

```
+ ~ host nice.software.
nice.software has address 213.212.81.71
+ ~ nslookup nice.software.
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   nice.software
Address: 213.212.81.71

+ ~
```

Vemos pela imagem que, de facto, o *host nice.software* existe porque tem o IP 213.212.81.71 associado. Para além de ser um *host*, também é um domínio porque responde à query de DNS realizada pelo *nslookup*.

- (e) Qual é o servidor DNS primário definido para o domínio *msf.org*? Este servidor primário (master) aceita queries recursivas? Porquê?

Para obter o servidor de DNS primário, fazemos uma query do tipo SOA ("*Start of Authority*"), que se vê na imagem que se segue:

```
+ ~ dig msf.org SOA

;<<>> DiG 9.16.1 <<>> msf.org SOA
;; global options: +cmd
;; Got answer:
;;->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8948
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;msf.org.      IN      SOA

;; ANSWER SECTION:
msf.org.      2560    IN      SOA     ns1.dds.nl. postmaster.msf.org. 1407464621 16384 2048 1048576 2560

;; AUTHORITY SECTION:
msf.org.      4880    IN      NS       ns2.dds.eu.
msf.org.      4880    IN      NS       ns4.dds-city.com.
msf.org.      4880    IN      NS       ns1.dds.nl.
msf.org.      4880    IN      NS       ns3.dds.amsterdam.

;; ADDITIONAL SECTION:
ns1.dds.nl.   4880    IN      A        91.142.253.70
ns2.dds.eu.   4880    IN      A        85.158.249.55
ns4.dds-city.com. 4880    IN      A        85.158.250.40

;; Query time: 139 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: dom abr 12 22:02:38 WEST 2020
;; MSG SIZE rcvd: 240

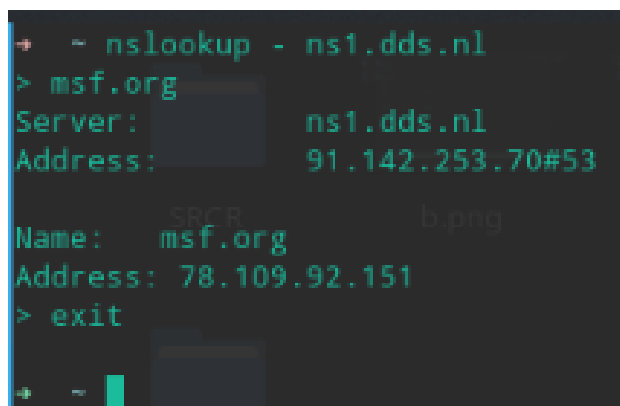
+ ~
```

Verificamos, então, que o servidor de DNS primário é **ns1.dds.nl**.

Para além disso, uma vez que a *flag ra* (*Recursion Available*) foi retornada significa que o servidor permite aos utilizadores queries recursivas.

(f) **Obtenha uma resposta “autoritativa” para a questão anterior**

Para obtermos uma resposta autoritativa temos de interrogar diretamente o servidor de DNS **ns1.dds.nl**, visto que é nele que se encontra o registo SOA para o nome *msf.org*.

A terminal window with a dark background and green text. The user enters the command 'nslookup - ns1.dds.nl' at the prompt. The prompt changes to '>'. The user then enters 'msf.org'. The terminal displays the following output: 'Server: ns1.dds.nl', 'Address: 91.142.253.70#53', 'Name: msf.org', and 'Address: 78.109.92.151'. The user then enters 'exit' and the prompt returns to the shell. There are some faint, semi-transparent text overlays on the terminal image, including 'SRGB' and 'b.png'.

Obtemos assim a confirmação que **msf.org** é parte do domínio de **ns1.dds.nl**.

(g) **Onde são entregues as mensagens de correio eletrónico dirigidas aos presidentes *marcelo@presidencia.pt* e *bolsonaro@casacivil.gov.br*?**

Como observação inicial, para **marcelo@presidencia.pt** temos o domínio **presidencia.pt** e para **bolsonaro@casacivil.gov.br** temos o domínio **casacivil.gov.br**.

Sabemos que o correio eletrónico é entregue no(a) servidor(es) MX (*Mail Exchanger*) associado(s) a cada um dos domínios. Procedemos, então, ao envio de interrogações MX para destacar estes servidores e obter os seus endereços.

- presidencia.pt:

```

→ ~ dig presidencia.pt MX
; <<>> DiG 9.16.1 <<>> presidencia.pt MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20316
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;presidencia.pt.                IN      MX

;; ANSWER SECTION:
presidencia.pt.                10800   IN      MX      10 mail2.presidencia.pt.
presidencia.pt.                10800   IN      MX      50 mail1.presidencia.pt.

;; AUTHORITY SECTION:
presidencia.pt.                6749    IN      NS      ns02.fcn.pt.
presidencia.pt.                6749    IN      NS      ns2.presidencia.pt.
presidencia.pt.                6749    IN      NS      ns1.presidencia.pt.

;; ADDITIONAL SECTION:
mail2.presidencia.pt.          10800   IN      A       192.162.17.32
mail1.presidencia.pt.          10800   IN      A       192.162.17.31
ns1.presidencia.pt.            6749    IN      A       192.162.17.5
ns02.fcn.pt.                   5995    IN      A       193.136.2.228
ns2.presidencia.pt.            6749    IN      A       192.162.17.6
ns02.fcn.pt.                   2744    IN      AAAA    2001:690:a80:4001::200

;; Query time: 19 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: seg abr 13 02:15:46 WEST 2020
;; MSG SIZE rcvd: 255
→ ~ █

```

Pelo que vemos na imagem, há dois registos MX com dois níveis distintos de preferência: 10 e 50. O que tem nível de preferência menor é aquele que será o servidor primário e o que tem maior será o secundário. Então:

- mail2.presidencia.pt.: servidor primário
- mail1.presidencia.pt.: servidor secundário

- casacivil.gov.br:

```

+ ~ dig casacivil.gov.br MX

; <<>> DiG 9.16.1 <<>> casacivil.gov.br MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15998
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;casacivil.gov.br.          IN      MX

;; ANSWER SECTION:
casacivil.gov.br.          3600    IN      MX      10 esa02.presidencia.gov.br.
casacivil.gov.br.          3600    IN      MX      5 esa01.presidencia.gov.br.

;; AUTHORITY SECTION:
casacivil.gov.br.          1718    IN      NS      alpha.planalto.gov.br.
casacivil.gov.br.          1718    IN      NS      alpha2.planalto.gov.br.

;; ADDITIONAL SECTION:
alpha.planalto.gov.br.     672     IN      A        170.246.255.10
alpha2.planalto.gov.br.    1219    IN      A        170.246.255.11

;; Query time: 313 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: seg abr 13 02:17:26 WEST 2020
;; MSG SIZE rcvd: 183

+ ~ █

```

Seguindo uma lógica semelhante ao anterior, temos dois níveis de preferência: 5 e 10. Então:

- esa01.presidencia.gov.br.: servidor primário
- esa02.presidencia.gov.br: servidor secundário

(h) Que informação é possível obter, via DNS, acerca de whitehouse.gov?

```

+ ~ dig www.whitehouse.gov

; <<>> DiG 9.16.1 <<>> www.whitehouse.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57113
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 8, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;www.whitehouse.gov.          IN      A

;; ANSWER SECTION:
www.whitehouse.gov. 300 IN CNAME wildcard.whitehouse.gov.edgekey.net.
wildcard.whitehouse.gov.edgekey.net. 900 IN CNAME e4036.dscb.akamaiedge.net.
e4036.dscb.akamaiedge.net. 20 IN A 23.10.65.110

;; AUTHORITY SECTION:
dscb.akamaiedge.net. 2878 IN NS n4dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n0dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n3dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n2dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n6dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n1dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n5dscb.akamaiedge.net.
dscb.akamaiedge.net. 2878 IN NS n7dscb.akamaiedge.net.

;; ADDITIONAL SECTION:
n3dscb.akamaiedge.net. 3533 IN A 2.16.65.215
n1dscb.akamaiedge.net. 2437 IN A 2.16.65.205
n2dscb.akamaiedge.net. 2058 IN A 2.16.65.207
n0dscb.akamaiedge.net. 2936 IN A 88.221.81.192
n5dscb.akamaiedge.net. 3984 IN A 2.16.65.214
n7dscb.akamaiedge.net. 1330 IN A 2.17.217.149
n6dscb.akamaiedge.net. 2454 IN A 88.221.53.221
n4dscb.akamaiedge.net. 3984 IN A 2.16.65.215
n0dscb.akamaiedge.net. 2878 IN AAAA 2600:1480:e800::c0

;; Query time: 93 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: seg abr 13 02:18:36 WEST 2020
;; MSG SIZE rcvd: 472

+ ~ █

```

Começando pela secção de respostas da query, verificamos que o IPv4 do nome *www.whitehouse.gov* é 23.10.65.110, obtido através das *aliases* (campo *CNAME*) deste. O nome *www.whitehouse.gov* é um *alias* de *wildcard.whitehouse.gov.edgekey.net* e *e4036.dscb.akamaiedge.net* é um *alias* de *wildcard.whitehouse.gov.edgekey.net*, cujo IPv4 é 23.10.65.110. A secção *AUTHORITY* indica os servidores que têm permissões de responder a queries sobre este domínio, que são os enumerados na imagem.

A secção adicional indica os IP's de todos os servidores na secção explicada imediatamente antes.

- (i) **Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a0-0:1036:1113::247 usando algum dos clientes DNS? Que informação consegue obter? Supondo que teve problemas com esse endereço, consegue obter um contacto do responsável por esse IPv6?**

É possível realizar interrogações DNS (neste caso fazemos uma interrogação usando o IPv6 e não o nome) usando o *nslookup*.

```
+ ~ nslookup 2001:690:a00:1036:1113::247
7.4.2.0.0.0.0.0.0.0.0.0.3.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      name = www.fccn.pt.

Authoritative answers can be found from:
6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns02.fccn.pt.
6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns01.fccn.pt.
ns02.fccn.pt      internet address = 193.136.2.228
ns01.fccn.pt      internet address = 193.136.192.40
ns02.fccn.pt      has AAAA address 2001:690:a80:4001::200
ns01.fccn.pt      has AAAA address 2001:690:a00:4001::200

+ ~
```

Obtemos, então, que o nome associado a este IPv6 é **www.fccn.pt**. Supondo que temos um problema com o endereço, temos de obter o endereço de correio eletrónico do domínio através de interrogações DNS do tipo SOA a **www.fccn.pt**.

```

→ ~ nslookup -type=soa fccn.pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
fccn.pt
    origin = ns01.fccn.pt
    mail addr = hostmaster.fccn.pt
    serial = 2020040802
    refresh = 21600
    retry = 7200
    expire = 1209600
    minimum = 14400

Authoritative answers can be found from:
fccn.pt nameserver = ns03.fccn.pt.
fccn.pt nameserver = ns01.fccn.pt.
fccn.pt nameserver = ns02.fccn.pt.
ns02.fccn.pt internet address = 193.136.2.228
ns03.fccn.pt internet address = 138.246.255.249
ns01.fccn.pt internet address = 193.136.192.40
ns02.fccn.pt has AAAA address 2001:690:a80:4001::200
ns03.fccn.pt has AAAA address 2001:4ca0:106:0:250:56ff:fea9:3fd
ns01.fccn.pt has AAAA address 2001:690:a00:4001::200

```

Concluindo, então, para contactarmos o responsável basta utilizarmos o endereço de email **hostmaster.fccn.pt**.

- (j) Os secundários usam um mecanismo designado por “Transferência de zona” para se atualizarem automaticamente a partir do primário, usando os parâmetros definidos no Record do tipo SOA do domínio. Descreve sucintamente esse mecanismo com base num exemplo concreto (ex: di.uminho.pt ou o domínio cc.pt que vai ser criado na topologia virtual).

O processo de transferência de zona é essencialmente o processo de replicação de uma base de dados de um servidor primário num servidor secundário, tipicamente induzido por uma query **AXFR**. Pegando num caso em concreto, utilizaremos o nome **di.uminho.pt**.


```

➔ ~ nslookup -type=SOA di.uminho.pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
di.uminho.pt
    origin = dns.di.uminho.pt
    mail addr = dnsadmin.di.uminho.pt
    serial = 2020040701
    refresh = 28800
    retry = 7200
    expire = 28800
    minimum = 43200

Authoritative answers can be found from:
di.uminho.pt    nameserver = alfa.di.uminho.pt.
di.uminho.pt    nameserver = dns3.uminho.pt.
di.uminho.pt    nameserver = dns.di.uminho.pt.
di.uminho.pt    nameserver = marco.uminho.pt.
di.uminho.pt    nameserver = dns2.uminho.pt.
di.uminho.pt    nameserver = ns3.eurotux.com.
di.uminho.pt    nameserver = dns2.di.uminho.pt.
di.uminho.pt    nameserver = ns1.eurotux.com.
di.uminho.pt    nameserver = dns.uminho.pt.
dns2.uminho.pt  internet address = 193.137.16.145
dns2.di.uminho.pt  internet address = 193.136.19.2
marco.uminho.pt internet address = 193.136.9.240
alfa.di.uminho.pt  internet address = 193.136.19.3
dns.uminho.pt  internet address = 193.137.16.75
ns1.eurotux.com internet address = 194.107.127.1
dns.di.uminho.pt  internet address = 193.136.19.1
dns3.uminho.pt  internet address = 193.137.16.65
ns3.eurotux.com internet address = 216.75.63.6
dns2.uminho.pt  has AAAA address 2001:690:2280:801::145
dns2.di.uminho.pt  has AAAA address 2001:690:2280:28::2
dns.uminho.pt  has AAAA address 2001:690:2280:1::75
dns.di.uminho.pt  has AAAA address 2001:690:2280:28::1
➔ ~ █

```

Ao realizar a query na imagem acima, notamos a presença de campos importantes na atualização automática do servidor secundário:

- **origin:** nameserver primário. Neste caso é *dns.di.uminho.pt*.
- **mail addr:** email do administrador da zona associada. Neste caso é *dnsadmin.di.uminho.pt*.

- **serial:** Permite saber a data da última alteração na base de dados do servidor primário. Se as datas diferirem, é porque a base de dados do secundário está desatualizada e, então, é realizado o processo de transferência de zona, ou seja, é enviada a nova cópia da base de dados para o secundário. Neste caso, vemos que a última alteração foi no dia 7 de abril de 2020 (foi também a primeira mudança).
- **refresh:** Indica a frequência a que deve ser verificado se as bases de dados foram alteradas (campo anterior). Neste caso em concreto, verificamos que é sempre que passam 28800 segundos (8 horas).
- **retry:** Se o servidor primário não responder quando é feito um pedido de *refresh*, este campo indica o tempo que deverá esperar até tentar novamente. Neste caso são 2 horas.
- **expire:** Indica o tempo que o servidor secundário permanece ativo se não forem respondidas os pedidos de *refresh* em períodos de *retry*. Neste caso fica ativo durante 8 horas e, quando passa esse tempo, o servidor pára de responder.
- **minimum:** Equivalente ao TTL, indica o tempo mínimo que os resultados de todo o processo de DNS ficam em cache. Neste caso, são apagados após 12 horas.

3 Parte 2

3.1 Servidor Primário

Para o servidor primário, construímos o ficheiro **db.cc.pt**, que contém toda informação dos registos dos nomes e IP's do nosso domínio **cc.pt**.

```
;  
$TTL 604800  
$ORIGIN pt.  
cc IN SOA dns.cc.pt. grupo02.cc.pt. (  
        3 ;Serial  
        604800 ;Refresh  
        86400 ;Retry  
        2419200 ;Expire  
        604800) ;Negative Cache TTL  
  
    IN NS  dns.cc.pt.  
    IN NS  dns2.cc.pt.  
    IN MX 10 mail.cc.pt.  
    IN MX 20 mail2.cc.pt.  
  
$ORIGIN cc.pt.  
    IN A   10.3.3.3  
dns     IN A   10.3.3.1  
dns2    IN A   10.4.4.1  
  
www     IN A   10.3.3.3  
mail    IN A   10.3.3.3  
  
pop     IN A   10.3.3.2  
imap    IN A   10.3.3.2  
mail2   IN A   10.3.3.2  
  
Portatil1 IN A   10.1.1.1  
Grupo02   IN CNAME Portatil1  
Portatil2 IN A   10.1.1.2  
Portatil3 IN A   10.1.1.3
```

Hermes	IN	CNAME	dns2
Zeus	IN	A	10.4.4.2
Atena	IN	A	10.4.4.3
Alfa	IN	A	10.2.2.1
Delta	IN	A	10.2.2.2
Omega	IN	A	10.2.2.3

Ou seja, associamos todos os sub-domínios (**mail.cc.pt**, **www.cc.pt**, etc) assim como os servidores de DNS.

Para os domínios reversos, necessitamos de ter em consideração as 4 sub-redes da topologia refere, isto é, as subredes 10.1.1.0/24, 10.2.2.0/24, 10.3.3.0/24 e 10.4.4.0/24.

```

zone "cc.pt" {
    type master;
    file "/home/core/primario/db.cc.pt";
    allow-transfer{ 10.4.4.1; };
};

zone "3.3.10.in-addr.arpa"{
    type master;
    file "/home/core/primario/db.3-3-10.rev";
    allow-transfer{ 10.4.4.1; };
};

zone "4.4.10.in-addr.arpa"{
    type master;
    file "/home/core/primario/db.4-4-10.rev";
    allow-transfer{ 10.4.4.1; };
};

zone "1.1.10.in-addr.arpa"{
    type master;
    file "/home/core/primario/db.1-1-10.rev";
    allow-transfer{ 10.4.4.1; };
};

```

```
};

zone "2.2.10.in-addr.arpa"{
    type master;
    file "/home/core/primario/db.2-2-10.rev";
    allow-transfer{ 10.4.4.1; };
};
```

Assim, os ficheiros **.rev** indicam precisamente o contrário dos **db**, fazem um mapeamento de IP's para nomes concretos.

Para a subrede 10.1.1.0/24:

```
;
$TTL      604800
1.1.10.in-addr.arpa.      IN      SOA      dns.cc.pt. grupo02.cc.pt. (
                           1          ; Serial
                           604800     ; Refresh
                           86400      ; Retry
                           2419200     ; Expire
                           604800 )   ; Negative Cache TTL

                           IN      NS      dns.cc.pt.
                           IN      NS      dns2.cc.pt.
$ORIGIN 1.1.10.in-addr.arpa.
1  IN  PTR Grupo02.cc.pt.
2  IN  PTR Portatil2.cc.pt.
3  IN  PTR Portatil3.cc.pt.
```

Para a subrede 10.2.2.0/24:

```
;
$TTL      604800
2.2.10.in-addr.arpa.      IN      SOA      dns.cc.pt. grupo02.cc.pt. (
                           1          ; Serial
                           604800     ; Refresh
                           86400      ; Retry
```

```

                                2419200      ; Expire
                                604800 )      ; Negative Cache TTL

                                IN      NS      dns.cc.pt.
                                IN      NS      dns2.cc.pt.
$ORIGIN 2.2.10.in-addr.arpa.
1  IN  PTR      Alfa.cc.pt.
2  IN  PTR      Delta.cc.pt.
3  IN  PTR      Omega.cc.pt.

Para a subrede 10.3.3.0/24:

;
$TTL      604800
3.3.10.in-addr.arpa.      IN      SOA      dns.cc.pt. grupo02.cc.pt. (
                                1      ; Serial
                                604800      ; Refresh
                                86400      ; Retry
                                2419200      ; Expire
                                604800 )      ; Negative Cache TTL

                                IN      NS      dns.cc.pt.
                                IN      NS      dns2.cc.pt.
$ORIGIN 3.3.10.in-addr.arpa.
1  IN  PTR      dns.cc.pt.

3  IN  PTR      www.cc.pt.
3  IN  PTR      mail.cc.pt.

2  IN  PTR      pop.cc.pt.
2  IN  PTR      imap.cc.pt.
2  IN  PTR      mail2.cc.pt.

```

Para a subrede 10.4.4.0/24:

```
;
```

```

$TTL      604800
4.4.10.in-addr.arpa.      IN      SOA      dns.cc.pt. grupo02.cc.pt. (
                           1          ; Serial
                           604800     ; Refresh
                           86400      ; Retry
                           2419200    ; Expire
                           604800 )   ; Negative Cache TTL

                           IN      NS      dns.cc.pt.
                           IN      NS      dns2.cc.pt.
$ORIGIN 4.4.10.in-addr.arpa.
1  IN  PTR      Hermes.cc.pt.
2  IN  PTR      Zeus.cc.pt.
3  IN  PTR      Atena.cc.pt.

```

3.2 Servidor Secundário

O servidor secundário é essencialmente um servidor que existe em caso de falha do primário, utilizando portanto as mesmas configurações, contudo, num endereço diferente.

Para criar este servidor essencialmente definimos os vários domínios reversos como sendo *slaves* assim como o próprio endereço **cc.pt**, isto é, obtém as informações que necessita referenciando um *master*, que é o servidor DNS primário, através de transferências dos ficheiros de dados e guardando em */var/cache/bind*.

```

zone "cc.pt" {
    type slave;
    file "/var/cache/bind/db.cc.pt";
    masters { 10.3.3.1; };
};

zone "3.3.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.3-3-10.rev";
    masters { 10.3.3.1; };
};

```

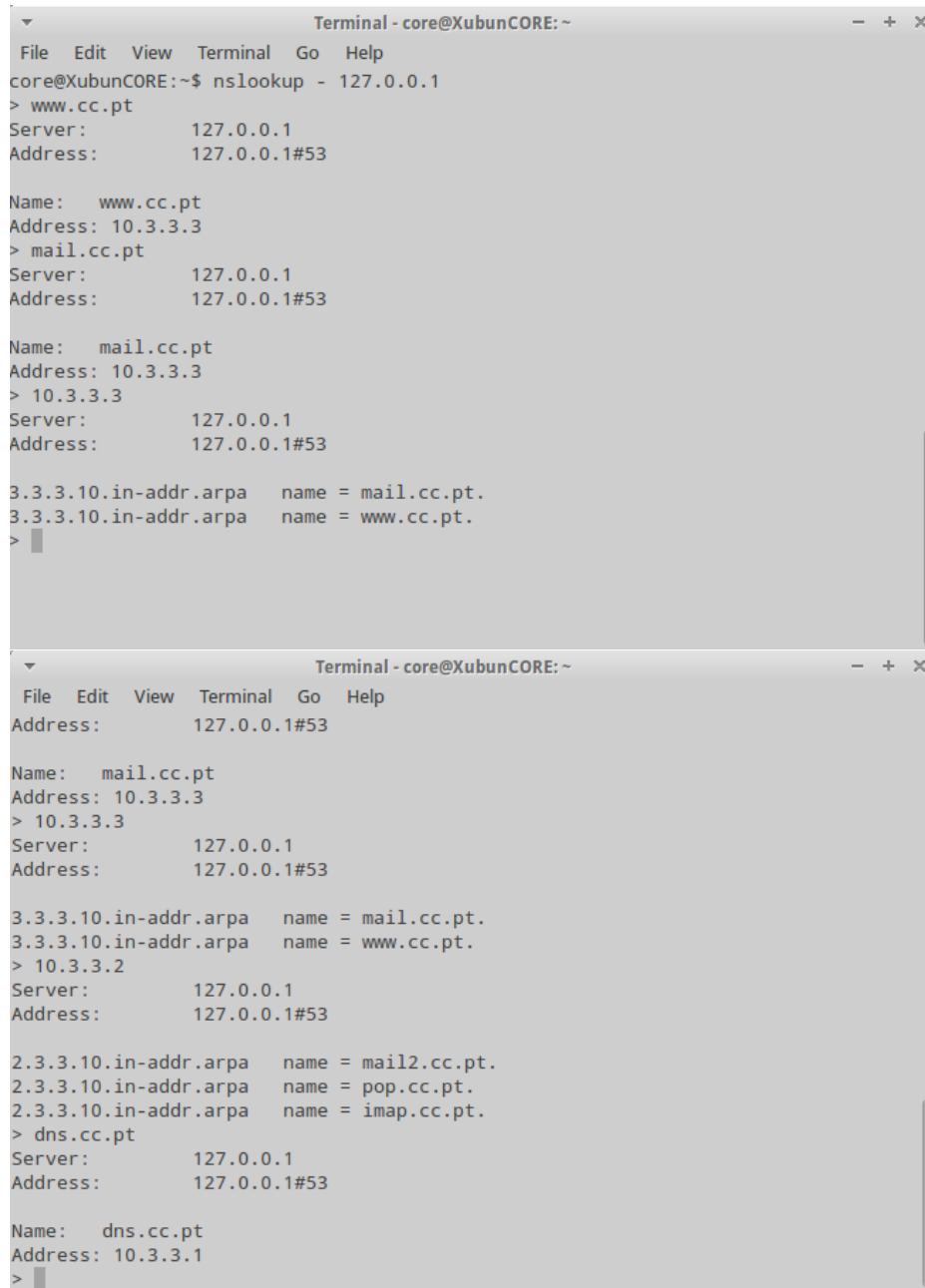
```
};

zone "4.4.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.4-4-10.rev";
    masters { 10.3.3.1; };
};

zone "1.1.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.1-1-10.rev";
    masters { 10.3.3.1; };
};

zone "2.2.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.2-2-10.rev";
    masters { 10.3.3.1; };
};
```


3.3 Testes e Demonstrações



The image shows two terminal windows from a user named 'core' on a system named 'XubunCORE'. Both windows are running the 'nslookup' command with the server set to '127.0.0.1'. The top window shows tests for 'www.cc.pt' and 'mail.cc.pt', both resolving to IP address 10.3.3.3. It also shows reverse lookups for 10.3.3.3 pointing to both domains. The bottom window continues the tests, showing reverse lookups for 10.3.3.2 pointing to 'mail2.cc.pt', 'pop.cc.pt', and 'imap.cc.pt', and a test for 'dns.cc.pt' which resolves to 10.3.3.1.

```
Terminal - core@XubunCORE: ~  
File Edit View Terminal Go Help  
core@XubunCORE:~$ nslookup - 127.0.0.1  
> www.cc.pt  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
Name:   www.cc.pt  
Address: 10.3.3.3  
> mail.cc.pt  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
Name:   mail.cc.pt  
Address: 10.3.3.3  
> 10.3.3.3  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
3.3.3.10.in-addr.arpa  name = mail.cc.pt.  
3.3.3.10.in-addr.arpa  name = www.cc.pt.  
>  
  
Terminal - core@XubunCORE: ~  
File Edit View Terminal Go Help  
Address:         127.0.0.1#53  
  
Name:   mail.cc.pt  
Address: 10.3.3.3  
> 10.3.3.3  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
3.3.3.10.in-addr.arpa  name = mail.cc.pt.  
3.3.3.10.in-addr.arpa  name = www.cc.pt.  
> 10.3.3.2  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
2.3.3.10.in-addr.arpa  name = mail2.cc.pt.  
2.3.3.10.in-addr.arpa  name = pop.cc.pt.  
2.3.3.10.in-addr.arpa  name = imap.cc.pt.  
> dns.cc.pt  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
Name:   dns.cc.pt  
Address: 10.3.3.1  
>
```

Testes em Localhost

```
root@Portatil1: /tmp/pycore.50205/Portatil1.conf
root@Portatil1:/tmp/pycore.50205/Portatil1.conf# nslookup - 10.3.3.1
> www.cc.pt
Server:      10.3.3.1
Address:     10.3.3.1#53

Name:   www.cc.pt
Address: 10.3.3.3
> 10.3.3.2
Server:      10.3.3.1
Address:     10.3.3.1#53

2.3.3.10.in-addr.arpa   name = pop.cc.pt.
2.3.3.10.in-addr.arpa   name = imap.cc.pt.
2.3.3.10.in-addr.arpa   name = mail2.cc.pt.
> █

root@Portatil1: /tmp/pycore.50205/Portatil1.conf
root@Portatil1:/tmp/pycore.50205/Portatil1.conf# nslookup www.cc.pt
Server:      10.3.3.1
Address:     10.3.3.1#53

Name:   www.cc.pt
Address: 10.3.3.3

root@Portatil1:/tmp/pycore.50205/Portatil1.conf# dig www.cc.pt

; <<>> DiG 9.8.1-P1 <<>> www.cc.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9476
;; flags: qr aa rd: QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.cc.pt.                IN      A

;; ANSWER SECTION:
www.cc.pt.                 604800  IN      A      10.3.3.3

;; AUTHORITY SECTION:
cc.pt.                     604800  IN      NS      dns2.cc.pt.
cc.pt.                     604800  IN      NS      dns.cc.pt.

;; ADDITIONAL SECTION:
dns.cc.pt.                 604800  IN      A      10.3.3.1
dns2.cc.pt.                604800  IN      A      10.4.4.1

;; Query time: 5 msec
;; SERVER: 10.3.3.1#53(10.3.3.1)
;; WHEN: Fri Apr 10 17:28:47 2020
;; MSG SIZE  rcvd: 112

root@Portatil1:/tmp/pycore.50205/Portatil1.conf# █
```

```
root@Portatil1: /tmp/pycore.53407/Portatil1.conf
> www.cc.pt
Server:      10.3.3.1
root@Portatil1:/tmp/pycore.53407/Portatil1.conf# nslookup - 10.3.3.1
> 10.4.4.3
Server:      10.3.3.1
Address:     10.3.3.1#53

3.4.4.10.in-addr.arpa  name = Atena.cc.pt.
> Atena.cc.pt
Server:      10.3.3.1
Address:     10.3.3.1#53

Name:  Atena.cc.pt
Address: 10.4.4.3
> Grupo02.cc.pt
Server:      10.3.3.1
Address:     10.3.3.1#53

Grupo02.cc.pt  canonical name = Portatil1.cc.pt.
Name:  Portatil1.cc.pt
Address: 10.1.1.1
> 10.1.1.1
Server:      10.3.3.1
Address:     10.3.3.1#53

1.1.1.10.in-addr.arpa  name = Grupo02.cc.pt.
> □
```

Testes ao Servidor Primário

```
root@Portatil3: /tmp/pycore.55546/Portatil3.conf
root@Portatil3:/tmp/pycore.55546/Portatil3.conf# nslookup - 10.4.4.1
> Omega.cc.pt
Server:      10.4.4.1
Address:     10.4.4.1#53

Name:  Omega.cc.pt
Address: 10.2.2.3
> 10.2.2.3
Server:      10.4.4.1
Address:     10.4.4.1#53

3.2.2.10.in-addr.arpa  name = Omega.cc.pt.
> 10.1.1.1
Server:      10.4.4.1
Address:     10.4.4.1#53

1.1.1.10.in-addr.arpa  name = Grupo02.cc.pt.
>

root@Portatil1: /tmp/pycore.53407/Portatil1.conf
root@Portatil1:/tmp/pycore.53407/Portatil1.conf# nslookup - 10.4.4.1
> www.cc.pt
Server:      10.4.4.1
Address:     10.4.4.1#53

Name:  www.cc.pt
Address: 10.3.3.3
> Grupo02.cc.pt
Server:      10.4.4.1
Address:     10.4.4.1#53

Grupo02.cc.pt  canonical name = Portatil1.cc.pt.
Name:  Portatil1.cc.pt
Address: 10.1.1.1
> 10.1.1.1
Server:      10.4.4.1
Address:     10.4.4.1#53

1.1.1.10.in-addr.arpa  name = Grupo02.cc.pt.
>
```

Testes ao Servidor Secundário

```

root@Hermes: /tmp/pycore.55546/Hermes.conf
15-Apr-2020 10:43:32.153 zone 2.2.10.in-addr.arpa/IN: sending notifies (serial 1)
15-Apr-2020 10:43:32.644 zone 3.3.10.in-addr.arpa/IN: Transfer started.
15-Apr-2020 10:43:32.644 zone 4.4.10.in-addr.arpa/IN: Transfer started.
15-Apr-2020 10:43:32.645 zone cc.pt/IN: zone transfer deferred due to quota
15-Apr-2020 10:43:32.646 zone 1.1.10.in-addr.arpa/IN: zone transfer deferred due to quota
15-Apr-2020 10:43:32.647 transfer of '3.3.10.in-addr.arpa/IN' from 10.3.3.1#53: connected using 10.4.4.1#33989
15-Apr-2020 10:43:32.649 transfer of '4.4.10.in-addr.arpa/IN' from 10.3.3.1#53: connected using 10.4.4.1#58057
15-Apr-2020 10:43:32.657 zone 3.3.10.in-addr.arpa/IN: transferred serial 1
15-Apr-2020 10:43:32.657 zone cc.pt/IN: Transfer started.
15-Apr-2020 10:43:32.657 transfer of '3.3.10.in-addr.arpa/IN' from 10.3.3.1#53: Transfer completed: 1 messages, 10 records, 273 bytes, 0.008 secs (34125 bytes/sec)
15-Apr-2020 10:43:32.658 zone 4.4.10.in-addr.arpa/IN: transferred serial 1
15-Apr-2020 10:43:32.658 zone 1.1.10.in-addr.arpa/IN: Transfer started.
15-Apr-2020 10:43:32.659 transfer of '4.4.10.in-addr.arpa/IN' from 10.3.3.1#53: Transfer completed: 1 messages, 7 records, 225 bytes, 0.009 secs (25000 bytes/sec)
15-Apr-2020 10:43:32.659 zone 3.3.10.in-addr.arpa/IN: sending notifies (serial 1)
15-Apr-2020 10:43:32.660 zone 4.4.10.in-addr.arpa/IN: sending notifies (serial 1)
15-Apr-2020 10:43:32.664 transfer of 'cc.pt/IN' from 10.3.3.1#53: connected using 10.4.4.1#41314
15-Apr-2020 10:43:32.664 transfer of '1.1.10.in-addr.arpa/IN' from 10.3.3.1#53: connected using 10.4.4.1#53148
15-Apr-2020 10:43:32.675 zone cc.pt/IN: transferred serial 3
15-Apr-2020 10:43:32.675 transfer of 'cc.pt/IN' from 10.3.3.1#53: Transfer completed: 1 messages, 24 records, 953 bytes, 0.011 secs (50272 bytes/sec)
15-Apr-2020 10:43:32.676 zone 1.1.10.in-addr.arpa/IN: transferred serial 1
15-Apr-2020 10:43:32.676 transfer of '1.1.10.in-addr.arpa/IN' from 10.3.3.1#53: Transfer completed: 1 messages, 7 records, 235 bytes, 0.012 secs (19583 bytes/sec)
15-Apr-2020 10:43:32.677 zone cc.pt/IN: sending notifies (serial 3)
15-Apr-2020 10:43:32.677 zone 1.1.10.in-addr.arpa/IN: sending notifies (serial 1)

```

Provas de Transferência do servidor secundário

4 Conclusão

Em suma, nesta segunda fase do trabalho, o grupo considera que já aparenta ter um conhecimento da matéria mais aprofundado sobre o DNS, nomeadamente na utilização e construção de *queries* (parte 1) e na criação do nosso próprio servidor de DNS (parte 2), embora num cenário mais controlado.

Foi dada a oportunidade de perceber o quão útil e importante é este serviço e o quanto dependemos dele, visto que uma ligeira alteração na maneira como nos ligamos a este serviço leva a resultados totalmente diferentes na resolução de nomes e IP's.

Por fim, por consequência dos anteriores percebemos o quão vulnerável estamos e o quão dependente estamos das boas intenções de quem gere os serviços, uma vez que o serviço de DNS, apesar dos servidores principais serem muito difíceis de atacar, é facilmente explorável nos computadores pessoais ou até mesmo redes locais.