

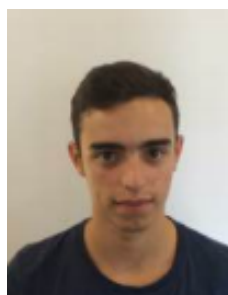


UNIVERSIDADE DO MINHO

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

Serviço de Resolução de Nomes (DNS)

TRABALHO PRÁTICO N.º 3



Alexandre Pacheco (A80760)

Diogo Sobral (A82523)

Inês Alves (A81368)

4 de Abril de 2019

Conteúdo

1	Questões e Respostas	2
1.1	<i>Pergunta a)</i>	2
1.2	<i>Pergunta b)</i>	2
1.3	<i>Pergunta c)</i>	3
1.4	<i>Pergunta d)</i>	4
1.5	<i>Pergunta e)</i>	5
1.6	<i>Pergunta f)</i>	6
1.7	<i>Pergunta g)</i>	7
1.8	<i>Pergunta h)</i>	8
1.9	<i>Pergunta i)</i>	9
1.10	<i>Pergunta j)</i>	10
2	Domínio de nomes CC.PT	11
3	Conclusão	14

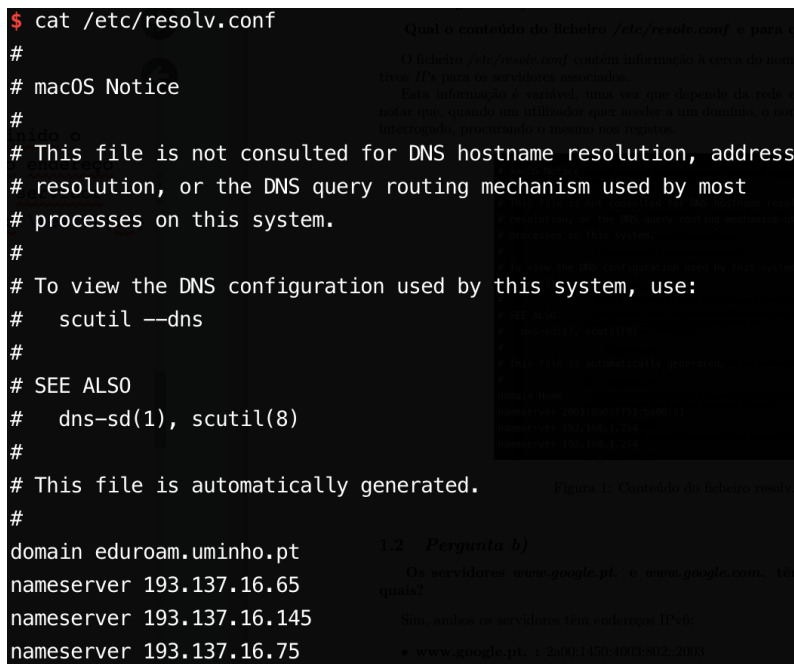
1 Questões e Respostas

1.1 Pergunta a)

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

O ficheiro `/etc/resolv.conf` contém informação sobre o nome do servidor DNS local e respetivos *IPs* para os servidores associados.

Esta informação é variável, uma vez que depende da rede em que o *host* se encontra. De notar que, quando um utilizador quer aceder a um domínio, o nome do servidor é o primeiro a ser interrogado, procurando o mesmo nos registos.



```
$ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
domain eduroam.uminho.pt
nameserver 193.137.16.65
nameserver 193.137.16.145
nameserver 193.137.16.75
```

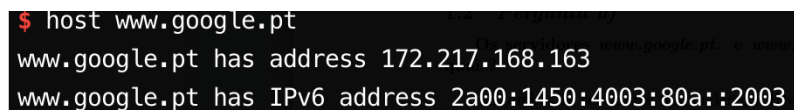
Figura 1: Conteúdo do ficheiro `resolv.conf`

1.2 Pergunta b)

Os servidores `www.google.pt.` e `www.google.com.` têm endereços IPv6? Se sim, quais?

Sim, ambos os servidores têm endereços IPv6:

- `www.google.pt.` : `2a00:1450:4003:802::2003`



```
$ host www.google.pt
www.google.pt has address 172.217.168.163
www.google.pt has IPv6 address 2a00:1450:4003:80a::2003
```

Figura 2: Endereço Ipv6 do servidor `www.google.pt.`

- **www.google.com.** : 2a00:1450:4003:802::2004

```
$ host www.google.com
www.google.com has address 172.217.16.228
www.google.com has IPv6 address 2a00:1450:4003:803::2004
```

Figura 3: Endereço Ipv6 do servidor www.google.com.

1.3 Pergunta c)

Quais os servidores de nomes definidos para os domínios: “ccg.pt.”, “pt.” e “.”?

Para o domínio “ccg.pt.” está definido o servidor *ns3.ccg.pt*, cujo endereço *IP* é 193.136.11.203, e o servidor *ns1.ccg.pt*, cujo endereço *IP* é 193.136.11.201.

```
$ nslookup
> set type=NS
> ccg.pt.
Server:          193.137.16.65
Address:         193.137.16.65#53

Non-authoritative answer:
ccg.pt  nameserver = ns1.ccg.pt.
ccg.pt  nameserver = ns3.ccg.pt.

Authoritative answers can be found from:
ns1.ccg.pt    internet address = 193.136.11.201
ns3.ccg.pt    internet address = 193.136.11.203
```

Figura 4: Servidores do domínio “ccg.pt.”

Por sua vez, para o domínio “pt.”, existem 10 servidores definidos. Para a representação dos mesmos, atentando à secção “Non-authoritative answer”, temos a seguinte imagem:

```
> pt.
Server:          193.137.16.65
Address:         193.137.16.65#53

Non-authoritative answer:
pt      nameserver = e.dns.pt.
pt      nameserver = b.dns.pt.
pt      nameserver = sns-pb.isc.org.
pt      nameserver = g.dns.pt.
pt      nameserver = a.dns.pt.
pt      nameserver = d.dns.pt.
pt      nameserver = c.dns.pt.
pt      nameserver = ns2.nic.fr.
pt      nameserver = ns.dns.br.
pt      nameserver = f.dns.pt.
```

Figura 5: Servidores do domínio “pt.”

Por fim, para o domínio ".", estão definidos 13 servidores. Seguindo o mesmo raciocínio do domínio anterior, os servidores deste estão representados a seguir.

```
> .
Server:      193.137.16.65
Address:     193.137.16.65#53

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

Figura 6: Servidores do domínio "."

1.4 Pergunta d)

Existe o domínio *eureka.software*.? Será que *eureka.software*. é um host?

Sim, o domínio *eureka.software*. existe, uma vez que tem correspondência. Este domínio não é um host, no entanto, é um servidor de e-mail. Esta conclusão pode ser comprovada executando o comando `"host eureka.software."`, que nos indica que este domínio se trata de um *alias*, tal como referido anteriormente, para um servidor de e-mail.

```
$ host eureka.software.
eureka.software has address 34.214.90.141
eureka.software mail is handled by 5 alt2.aspmx.l.google.com.
eureka.software mail is handled by 10 aspmx3.googlemail.com.
eureka.software mail is handled by 1 aspmx.l.google.com.
eureka.software mail is handled by 10 aspmx2.googlemail.com.
eureka.software mail is handled by 5 alt1.aspmx.l.google.com.
```

Figura 7: Execução do comando "host eureka.software"

1.5 Pergunta e)

Qual é o servidor DNS primário definido para o domínio *ami.pt*? Este servidor primário (master) aceita *queries* recursivas? Porquê?

O servidor DNS primário definido para o domínio *ami.pt* é o servidor "*ns1.dot2web.com*". Mais uma vez, atentando na secção "*Non-authoritative answer*" e, por sua vez, na sub-secção "*origin*", podemos corroborar a resposta dada.

```
$ nslookup
> set type=SOA
> ami.pt.
Server:          193.137.16.65
Address:         193.137.16.65#53

Non-authoritative answer:
ami.pt
    origin = ns1.dot2web.com
    mail addr = dc.dot2web.pt
    serial = 2019040100
    refresh = 3600
    retry = 7200
    expire = 1209600
    minimum = 86400
```

Figura 8: Execução do comando "nslookup" do tipo SOA para o domínio *ami.pt*.

Este servidor primário aceita *queries* recursivas, uma vez que, ao ser executado o comando "*dig ns1.dot2web.com*", obtemos o seguinte resultado:

```
$ dig ns1.dot2web.com

; <<>> DiG 9.10.6 <<>> ns1.dot2web.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33556
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
;; QUESTION SECTION:
;ns1.dot2web.com.                IN      A
;; ANSWER SECTION:
ns1.dot2web.com.                3590    IN      A      80.172.230.28
```

Figura 9: Execução do comando "dig ns1.dot2web.com"

Analisando esta imagem, repare-se que o servidor contém a *flag* "ra" (Recursion Available), o

que nos indica que há recursividade neste servidor.

1.6 Pergunta f)

Obtenha uma resposta “autoritativa” para a questão anterior.

Com o intuito de obter uma resposta “autoritativa” para a questão anterior, foi executado o comando *nslookup* do tipo SOA, que nos forneceu o seguinte resultado:

```
> set type=SOA
> ami.pt.
Server:          193.137.16.65
Address:         193.137.16.65#53
Non-authoritative answer:
ami.pt
      origin = ns1.dot2web.com
      mail addr = dc.dot2web.pt
      serial = 2019040100
      refresh = 3600
      retry = 7200
      expire = 1209600
      minimum = 86400
Authoritative answers can be found from:
ami.pt nameserver = ns1.ami.pt.
ami.pt nameserver = ns2.ami.pt.
ns1.ami.pt internet address = 80.172.230.28
ns2.ami.pt internet address = 5.199.172.41
> server ns1.ami.pt
Default server: ns1.ami.pt
Address: 80.172.230.28#53
> ami.pt.
;; connection timed out; no servers could be reached
> ami.pt.
```

Figura 10: Execução do comando *nslookup* do tipo SOA para o domínio *ami.pt*. II

Ora, com isto, obtivemos os seguintes endereços autoritativos: *ns1.ami.pt.* e *ns2.ami.pt.*. Para obtermos uma resposta autoritativa, é necessário questioná-los. Consequentemente, foi executado “*server ns1.ami.pt*”, selecionando, assim, este servidor.

Agora, questionando o servidor selecionado, novamente com “*ami.pt.*”, obtivemos como resposta “*connection timed out*”, uma vez que apenas um servidor local admite responder em modo recursivo ao cliente.

1.7 Pergunta g)

Onde são entregues as mensagens dirigidas a *marcelo@presidencia.pt*? E a *guterres@onu.org*?

Para obter os servidores que irão tratar de gerir os e-mails enviados temos que executar os comandos descritos nas imagens abaixo:

```
$ nslookup
> set type=MX
> presidencia.pt
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
presidencia.pt mail exchanger = 10 mail2.presidencia.pt.
presidencia.pt mail exchanger = 50 mail1.presidencia.pt.
```

Figura 11: Servidores de mail para a presidência.

```
$ nslookup
> set type=MX
> onu.org
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
onu.org mail exchanger = 10 mail.onu.org.
```

Figura 12: Servidores de mail para a onu.

Neste sentido, as mensagens para *guterres@onu.org* serão entregues em *mail.onu.org*. Ao contrário dos servidores da ONU, a presidência possui duas opções. Uma vez que *mail2.presidencia.pt* tem o valor 10, sendo este inferior a 50, significa que este servidor é o prioritário. Assim, a mensagem será entregue em *mail2.presidencia.pt* e, caso este não esteja disponível, a mensagem tentará ser entregue no *mail1.presidencia.pt*.

1.8 Pergunta h)

Que informação é possível obter acerca de *www.whitehouse.gov*? Qual é o endereço IPv4 associado?

Executando o comando "dig www.whitehouse.gov" obtivemos o seguinte resultado:

```
$ dig www.whitehouse.gov
; <=> DiG 9.10.6 <=> www.whitehouse.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37908
;; 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
```

Figura 13: Execução do comando "dig www.whitehouse.gov"@"

Atentando à secção "Answer Section", podemos ver que o endereço "www.whitehouse.gov." possui um alias para "wildcard.whitehouse.gov.edgekey.net." e este, por sua vez, tem um alias para "e4036.dscb.akamaiedge.net.". Por fim, este tem ainda um endereço IP associado.

Analisando esta informação, é fácil concluir que, com todas estas relações, então, o endereço "www.whitehouse.gov", possui o mesmo endereço IP de "e4036.dscb.akamaiedge.net.": 23.10.65.110, sendo este o endereço IPv4 pedido no enunciado.

1.9 Pergunta i)

Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::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?

Sim, usando o comando *nslookup*. A partir desta execução, com o tipo PTR, realiza *reverse mapping* e obtemos o domínio associado ao endereço IP fornecido. 2001:690:a00:1036:1113::247.

```
$ nslookup
> set type=PTR
> 2001:690:a00:1036:1113::247
Server: 193.137.16.65
Address: 193.137.16.65#53
Non-authoritative answer:
7.4.2.0.0.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa name = www.fccn.pt.
DNS? Que informação consegue obter? Supondo que teve problemas com esse endereço
Authoritative answers can be found from:
0.9.6.0.1.0.0.2.ip6.arpa nameserver = ns02.fccn.pt.
0.9.6.0.1.0.0.2.ip6.arpa nameserver = ns01.fccn.pt.
0.9.6.0.1.0.0.2.ip6.arpa nameserver = ns03.fccn.pt.
ns01.fccn.pt internet address = 193.136.192.40
ns02.fccn.pt internet address = 193.136.2.228
ns01.fccn.pt has AAAA address 2001:690:a00:4001::200
```

Figura 14: Execução do comando "nslookup" do tipo PTR

Posto isto, conseguimos concluir que o domínio que equivale a este endereço IP é *www.fccn.pt.*. Com esta informação, realizamos outra *query* sobre este domínio, do tipo SOA, identificando os seus contactos responsáveis. Como resultado obtivemos a figura seguinte, que nos mostra que o servidor responsável é *ns01.fccn.pt.*

```
> set type=SOA
> www.fccn.pt.
Server: 193.137.16.65
Address: 193.137.16.65#53
Non-authoritative answer:
*** Can't find www.fccn.pt.: No answer
Authoritative answers can be found from:
fccn.pt
origin = ns01.fccn.pt
mail addr = hostmaster.fccn.pt
serial = 2019040301
refresh = 21600
retry = 7200
expire = 1209600
minimum = 14400
```

Figura 15: Demonstração do servidor responsável

1.10 Pergunta 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).

A transferência de zona DNS é um tipo de transação de DNS. É um dos muitos mecanismos disponíveis para os administradores replicarem bases de dados DNS num conjunto de servidores DNS. Uma transferência de zona usa o TCP para transporte e assume a forma de uma transação cliente-servidor.

O cliente solicita uma transferência de dados de um servidor primário para um servidor secundário. À parte da base de dados que é replicada dá-se o nome de zona.

Através dos parâmetros definidos no Record do tipo SOA (Start of Authority) e fazendo uso do domínio cc.pt que foi criado na topologia virtual, podemos obter as seguintes informações:

```
$TTL      604800
@         IN      SOA      dns.cc.pt grupo49.cc.pt. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
```

Figura 16: Conteúdo do ficheiro resolv.conf

- **Serial:** número de série da zona. Se o servidor secundário associado a este observar uma diminuição deste número, então assume que a zona está desatualizada e inicia-se uma transferência de zona;
- **Refresh:** número de segundos após o qual o servidor secundário deve contactar o servidor primário para atualizar informações, a fim de detetar alterações de zona;
- **Retry:** após uma tentativa falhada, número de segundos que o servidor secundário deve esperar até tentar uma reconexão com o servidor primário. Este tempo deve ser inferior ao tempo do parâmetro *refresh*;
- **Expire:** número de segundos após o qual o servidor secundário deve parar de fazer solicitações para a zona em questão, se o servidor primário não responder. Este valor deve ser maior do que a soma do valor dos parâmetros *refresh* e *retry*.

Concluindo, o servidor secundário deverá contactar o servidor primário para tomar conhecimento de possíveis mudanças após 7 dias (604800 segundos) terem passado; que o mesmo espera 1 dia (86400 segundos) até voltar a tentar realizar a conexão ao servidor primário, após uma tentativa de conexão falhada. Se o servidor primário não responder, o servidor ainda tenta, periodicamente, obter uma resposta até 28 dias (2419200 segundos), mas, depois desse tempo ser esgotado, a base de dados secundária deixa de tentar conectar-se com a primária.

2 Domínio de nomes CC.PT

Durante a execução das instruções presentes no guião, podemos afirmar que houve alturas em que nos limitávamos a seguir o enunciado, mas também nos debruçamos sobre situações em que as instruções do guião necessitaram de ser complementadas com tomadas de decisões da nossa parte e serão essas o principal foco desta secção.

A primeira vez que tivemos que complementar o problema deu-se ao editar o ficheiro *primario/named.conf*. Uma vez que a topologia CC-MIEI 2019 detém 4 redes LAN diferentes, decidimos que, ao invés que apenas colocar as zonas *cc.pt* e *1.1.10.in-addr.arpa* no ficheiro, devíamos colocar uma zona para cada rede LAN diferente. Neste sentido, o ficheiro *primario/named.conf* ficou com 5 zonas após adicionarmos as zonas *2.2.10.in-addr.arpa*, *3.3.10.in-addr.arpa* e *4.4.10.in-addr.arpa*. Ao definir cada zona, foi necessário utilizar usar o *type master* para cada uma, visto que estávamos a mexer nas zonas do servidor DNS principal.

A esta informação foi ainda necessário adicionar a cláusula *allow-transfer {10.2.2.3;}* de modo a permitir a transferência para o servidor secundário e adicionar o ficheiro na respetiva base de dados.

Após a configuração das zonas, seguiu-se a criação e a configuração do ficheiro *db.cc.pt*. Aqui o primeiro passo foi a configuração do Start of Authority(SOA). Escolhemos o *dns.cc.pt* para a posição do DNS principal desta zona, visto que este é o servidor principal e, para o lugar do administrador, usamos o *grupo49.cc.pt*, por ser um dos requisitos mencionados no enunciado.

```
@      IN      SOA      dns.cc.pt grupo49.cc.pt. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
```

Figura 17: Introdução do SOA na base de dados

Após o SOA, introduzimos os *nameservers dns.cc.pt* e *dns2.cc.pt* utilizando o *type NS*. A estes seguiram-se os servidores de e-mail *mail.cc.pt* e *Servidor2.cc.pt*, mas, desta vez, dando uso à cláusula MX.

```
@      IN      NS      dns.cc.pt.
@      IN      NS      dns2.cc.pt.
@      IN      MX      10     mail.cc.pt.
@      IN      MX      20     Servidor2.cc.pt.
```

Figura 18: Introdução dos servidores de mail e name servers

É de notar que, como podemos observar na imagem acima apresentada, ambos os servidores de e-mail possuem um número que é responsável pela prioridade, sendo que, quando maior este número, menos prioritário será. Como o servidor primário de e-mail é o *mail.cc.pt* este possui um valor inferior ao do *Servidor2.cc.pt*.

Para todos os elementos, inserimos um registo com o nome do elemento na topologia e o respetivo endereço recorrendo ao tipo A, seguindo a seguinte regra:

(Nome do elemento na Topologia) IN A (Endereço IP)

Deste modo, conseguimos executar o comando *ping* (Nome na Topologia).cc.pt para todos os elementos presentes na topologia e ainda resolvemos os requisitos Alfa.cc.pt, Beta.cc.pt e Gama.cc.pt.

Servidor2	IN	A	10.1.1.2
Servidor3	IN	A	10.1.1.3
Servidor1	IN	A	10.1.1.1
Alfa	IN	A	10.3.3.1
Beta	IN	A	10.3.3.2
Gama	IN	A	10.3.3.3
Urano	IN	A	10.2.2.3
Neptuno	IN	A	10.2.2.2
Plutao	IN	A	10.2.2.1
Cliente3	IN	A	10.4.4.3
Cliente2	IN	A	10.4.4.2
Cliente1	IN	A	10.4.4.1

Figura 19: Mapping para todos os elementos da topologia.

Tal como fizemos acima, agora é necessário fazer o mesmo para os serviços necessários. Assim, utilizando a mesma regra e substituindo o nome do elemento na topologia pelo nome do elemento no serviço, fizemos o *mapping* para os serviços.

(Nome do elemento no Serviço) IN A (Endereço IP)
--

mail	IN	A	10.1.1.3
pop	IN	CNAME	Servidor2
imap	IN	CNAME	Servidor2
www	IN	A	10.1.1.3
dns	IN	A	10.1.1.1
dns2	IN	A	10.2.2.3

Figura 20: Mapping para todos os serviços.

Por fim, para estabelecer o alias entre Cliente1.cc.pt e Grupo49.cc.pt usamos a seguinte cláusula:

Grupo49 IN CNAME Cliente1

Figura 21: Cliente1.cc.pt alias Grupo49.cc.pt

Após o fecho da configuração da db.cc.pt, iniciamos o processo para configurar todos os ficheiros de domínios reverse. Embora houvesse a necessidade de configurar 4 ficheiros diferentes, o procedimento acabou por ser semelhantes para os 4 casos. Definimos o mesmo SOA que em db.cc.pt para os 4 ficheiros e apenas adicionamos os 2 *nameservers* existentes, *dns.cc.pt* e *dns2.cc.pt*.

Para todos os elementos presentes em cada LAN foi adicionada uma entrada na base de dados no ficheiro da rede correspondente, seguindo a seguinte regra:

(Valor da interface da rede) IN PTR (Nome do elemento na Topologia).cc.pt.
--

A estas entradas foi ainda necessário adicionar o *reverse mapping* para os serviço e para todos os alias.

```

$TTL      604800
@         IN      SOA      dns.cc.pt grupo49.cc.pt. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       dns.cc.pt.
@         IN      NS       dns2.cc.pt.

1         IN      PTR      Cliente1.cc.pt.
2         IN      PTR      Cliente2.cc.pt.
3         IN      PTR      Cliente3.cc.pt.
1         IN      PTR      Grupo49.cc.pt.

```

Figura 22: Exemplo do reverse mapping para a rede 10.4.4.0/24

No fim de definir as 4 bases de dados para o domínio reverse, a configuração do servidor DNS primário ficou concluída.

Na configuração do servidor secundário, apenas foi necessário adicionar as zonas definidas no servidor primário, com algumas alterações nas cláusulas usadas no ficheiro *named.conf*. O *type* que outrora fora *master* tomou o valor de *slave* e o *allow-transfer* foi substituído por *masters{ 10.1.1.1; }*. O path para o ficheiro também foi atualizado.

```

zone "cc.pt" {
    type slave;
    file "/var/cache/bind/db.cc.pt";
    masters { 10.1.1.1; };
};

zone "1.1.10.in-addr.arpa" {
    type slave;
    file "/var/cache/bind/db.1-1-10.rev";
    masters { 10.1.1.1; };
};

zone "2.2.10.in-addr.arpa" {
    type slave;
    file "/var/cache/bind/db.2-2-10.rev";
    masters { 10.1.1.1; };
};

zone "3.3.10.in-addr.arpa" {
    type slave;
    file "/var/cache/bind/db.3-3-10.rev";
    masters { 10.1.1.1; };
};

zone "4.4.10.in-addr.arpa" {
    type slave;
    file "/var/cache/bind/db.4-4-10.rev";
    masters { 10.1.1.1; };
};

```

Figura 23: Ficheiro secundario/named.conf

3 Conclusão

Terminado este 3.º Trabalho Prático, é seguro afirmarmos que conseguimos, enquanto grupo, aprofundar os nossos conhecimentos no âmbito das Comunicações por Computador, pondo em prática os conteúdos que aprendemos nas aulas teóricas desta Unidade Curricular.

Posto isto, apresentamos, como resultado final deste projeto, ambos os servidores propostos, primário e secundário, devidamente funcionais. Apesar das dificuldades encontradas aquando de todo o desenvolvimento deste trabalho, o grupo superou-as com distinção e todos os propósitos iniciais foram alcançados, revelando um trabalho consistente e bem estruturado.